NOTE TO USERS

A SURVEY OF RESULTS ON GIUGA'S CONJECTURE AND RELATED CONJECTURES

by

Joseph R. Hobart

BSc., University of Northern British Columbia, 2004

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
in
MATHEMATICAL, COMPUTER AND PHYSICAL SCIENCES
(MATHEMATICS)

THE UNIVERSITY OF NORTHERN BRITISH COLUMBIA

July 2005

Your file Votre référence
ISBN: 978-0-494-28392-9
Our file Notre référence
ISBN: 978-0-494-28392-9

APPROVAL

Name: Joseph hobart

Degree: Master of Science

Thesis Title: CONJECTURAL PRIME TESTS USING BERNOULLI NUMBERS AND THE RIEMANN ZETA FUNCTION

Examining Committee:

Chair: Dr. Kenneth Prkachin, Professor
Psychology Program
University of Northern British Columbia

Co-Supervisor: Dr. Lee Keener, Professor
Mathematical, Computer, and Physical Sciences Program
University of Northern British Columbia

Co-Supervisor: Dr. Patrick Montgomery, Associate Professor
Mathematical, Computer, and Physical Sciences Program
University of Northern British Columbia

Committee Member: Dr. Charles Brown, Associate Professor
Mathematical, Computer, and Physical Sciences Program
University of Northern British Columbia

External Examiner: Dr. Karl Dilcher, Professor
Department of Mathematics and Statistics
Dalhousie University

Date Approved: August 31, 2005

Abstract

In 1950, G. Giuga developed a method of determining if a natural number n is prime [20];

$$n \text{ is prime } \iff \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}.$$

Giuga proved his conjecture up to 1000 digits. However, he was unable to extend his proof to all natural numbers.

Thirty-five years later, in 1985, E. Bedocchi extended Giuga's result to 1700 digits [6]. More recently, Borwein et al extended Giuga's result to 13,800 digits [8]; however, they were unable to prove the conjecture.

Since all previous attempts to prove the conjecture failed, researchers attempted to reformulate Giuga's conjecture. The first published attempt was by Agoh in 1991. Agoh's reformulation

$$n \text{ is prime } \iff nB_{n-1} \equiv -1 \pmod{n},$$

became known as Agoh's conjecture [2]. Concurrently, a 1994 thesis by Wong showed 8 variations on Giuga's conjecture using different combinations of $\phi(n)$ in place of $n-1$ [57].

This thesis attempts to detail every known result on Giuga's conjecture. By consolidating all published results along with some unpublished results we hope to aid those who wish to study Giuga's conjecture in the future.

Contents

List of Figures

List of Tables

Acknowledgements

First, I would like to thank Dr. Lee Keener for taking the time to teach so many extra courses on top of his paid workload. If not for the course MATH 499 - Special Topics in Number Theory, I would never have had an opportunity to first learn about Giuga's Conjecture. I would also like to thank him for his infinite patience while I changed my mind (several times) not only on my thesis topic but my mathematical direction in general.

Next, but certainly by no means less valuable, were the comments and corrections given by my supervisory committee of Dr. Patrick Montgomery and Dr. Keener. The time that they spent teaching me to refine my ideas and methodology (and my writing) was by far the most important lesson I learned from UNBC. I would also like to acknowledge and thank my committee members, Dr. Charles Grant Brown and Dr. Karl Dilcher for their assistance completing my thesis defense.

I would also like to thank my friends, family, instructors (especially Edward Dobrowolski) and fellow graduate students. Without their constant support and coercing, I might still be writing this paper.

1 Introduction

Number theory is one of the fastest growing areas of mathematics. Useful applications of number theory in other areas of mathematics are becoming increasingly numerous. For instance, results in cryptography and the theory of elliptic curves are often first seen in number theory. For years, however, mathematicians viewed number theory, not as a tool for solving problems on a larger stage, but as an example of mathematical beauty. When asked what practical applications number theory could provide to everyday people, number theorists were often heard to answer, "None."

There are still areas of number theory which seem to be fruitless from a practical point of view. Bernoulli numbers, Euler polynomials, quadratic residues and many other aspects of classical number theory might fit this mold. This is not the case. It will be shown that Bernoulli numbers (and therefore Euler polynomials) can be used as prime testing mechanisms, while it is already known that quadratic residues can be used to factor and are often the underlying theory in different cryptographic applications.

This thesis extends what is known with respect to Giuga's conjecture.

$$n \text{ is prime } \iff \sum_{k=1}^{n} k^{n-1} \equiv -1 \pmod{n}.$$

The thesis is a complete compilation of published results on Giuga's conjecture while also discussing many of the topics underlining the conjecture and possible counterexamples.

The thesis begins with a brief review of basic number theory, classical number theory, algebra, numerical analysis, prime testing and factoring. This chapter (Chapter 2) serves simply as a reference for what is to follow in the remaining chapters. Material found in this chapter can also be found in [1], [19], [22], [25], [35], [36], [37],

[39] and [41]. For material on prime testing and factoring, the reader is urged to read [4], [5], [10], [12], [17], [24], [25], [27], [30], [34], [44] and [56].

The third chapter looks at the known results on Giuga's conjecture. Most of the material can be found in [2], [6], [8], [20], [23], [36], [37] and [57]. Some new results will also appear.

Number theory is a beautiful branch of mathematics and indeed of science as a whole. Its beauty is often overshadowed by its ever increasing applicability to real life problems. This thesis, despite my best efforts, continues this overshadowing. It is my hope that eventually Giuga's conjecture is proved and will become the basis for a new prime test.

2 Background Material

"Mathematics is the language with which God wrote the universe."

- Galileo Galilei -

This chapter serves only as a reference for what is to follow in this thesis. We begin with some basic notation. Define the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ in the usual way. To avoid confusion, please note that $\mathbb{N} = \mathbb{Z}^+ \cup \{0\}$. Also, Define $\mathbb{P}$ to be the set of all prime numbers.

2.1 Number Theory

All results in this section are standard and can be found in any number theory text, for example [38] and [22]. One of the most basic concepts in number theory is that of divisibility and divisors.

Definition 2.1 *For $a \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$, we say that a divides n, written $a|n$, if there exists $b \in \mathbb{Z}$ such that $ab = n$. If no such b exists, we say that $a \nmid n$.*

Theorem 2.1 (Euclid's Lemma) *If p is a prime, and $p|ab$, then $p|a$ or $p|b$ or both.*

Definition 2.2 *We say that a^m exactly divides n if $a^m|n$ but, $a^{m+1} \nmid n$. We denote a^m exactly divides n by $a^m||n$.*

Definition 2.3 *An integer n is said to be b-smooth if n has no prime factors larger than b.*

Definition 2.4 *We say that a is congruent to b modulo n, denoted by*

$$a \equiv b \pmod{n},$$

if $n|(a-b)$. *If* $a \equiv b \pmod{n}$, *then* a *and* b *are said to be in the same residue class modulo* n.

The following is a consequence of considering residue classes modulo n [8].

Theorem 2.2

$$\sum_{k=1}^{p-1} k^{n-1} \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1)|(n-1) \\ 0 \pmod{p} & \text{otherwise.} \end{cases} \tag{1}$$

Definition 2.5 *For* $a, b \in \mathbb{N}$, *we define the greatest common divisor of* a *and* b, *denoted* (a, b) *as the largest positive integer* n *such that* $n|a$ *and* $n|b$.

Definition 2.6 *The least common multiple of two positive integers,* a *and* b, *is the smallest* $n \in \mathbb{Z}^+$ *such that* $a|n$ *and* $b|n$. *We denote the least common multiple by* $lcm(a, b)$.

The following theorem relates the greatest common divisor to the least common multiple [38].

Lemma 2.1 *Let* $a, b \in \mathbb{N}$. *Then,*

$$(a, b) \cdot lcm(a, b) = ab.$$

One of the key observations about the greatest common divisor of a and b is that any linear combination of a and b can be expressed as a multiple of (a, b).

Theorem 2.3 *Suppose that* $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}$, *and* $(a, b) = n$, *then there exists integers* x *and* y *such that*

$$ax + by = n.$$

That is, there is a linear combination of a *and* b *equal to* (a, b).

Generally, in analytic number theory, we are concerned about integers. Thus, for equations, we generally only pay attention to integral solutions (solutions in integers). This makes the following observation very important [38].

Corollary 2.1 *Given a, b, $c \in \mathbb{Z}$, the Diophantine equation $ax + by = c$ has integral solutions iff $(a, b)|c$.*

We can go further and state the following theorem [38].

Theorem 2.4 *Take $a, b, c \in \mathbb{Z}$. Set $h = (a, b)$. Since $a = uh$ and $b = vh$, then the equation $ax + by = c$ has no integral solutions unless $h|c$. Moreover, the general integral solution of the equation is $x = x_0 - vk$, $y = y_0 + uk$, $k \in \mathbb{Z}$ where (x_0, y_0) is a particular solution.*

Another well-known and fundamental theorem of number theory is due to Fermat. The proof of Fermat's Little Theorem can be found in any introductory number theory textbook, for example Koblitz [25].

Theorem 2.5 (Fermat's Little Theorem) *Let $a \in \mathbb{Z}^+$ and $p \in \mathbb{P}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

The following theorem can be found in Wong [57]. It relates powers modulo prime powers.

Lemma 2.2 *Let $a \in \mathbb{Z}^+$ and $p \in \mathbb{P}$. For every $i \in \mathbb{N}$, if $a \equiv 1 \pmod{p}$ then $a^{p^i} \equiv 1 \pmod{p^{i+1}}$.*

We conclude with the definition of Euler's totient function (also called the phi function).

Definition 2.7 *Let $n \in \mathbb{Z}^+$. Then $\phi(n)$ is the number of integers k, with $1 \leq k \leq n$ such that $(n, k) = 1$.*

Basic properties of the totient function can be found in any introductory number theory book, for example Bressoud and Wagon [11].

Though this is only a brief introduction, the bulk of what is used later has been covered already. Any additional results used later will be stated as required.

2.2 Abstract Algebra

There are many good abstract algebra textbooks. Among them, Gallian's book [19] is the main reference for the following results.

Definition 2.8 *A **group** G is defined to be a set (finite or infinite) along with a binary operation $\bigoplus$ on G which assigns to each pair (a, b) of elements in G an element denoted by $a \bigoplus b$, with following properties:*

- ***closure**: If $a, b \in G$ then $a \bigoplus b \in G$,*
- ***associativity**: If $a, b, c \in G$ then $(a \bigoplus b) \bigoplus c = a \bigoplus (b \bigoplus c)$,*
- ***identity**: There is a unique element $I \in G$ such that $a \bigoplus I = a = I \bigoplus a$,*
- ***inverse**: For every $a \in G$ there is a unique a^{-1} such that $a \bigoplus a^{-1} = I = a^{-1} \bigoplus a$.*

If for all $a, b \in G$, $a \bigoplus b = b \bigoplus a$, the group is said to be commutative or abelian.

Example 1 *It is not difficult to show that the following sets under the indicated operation form groups:*

- $\mathbb{Z}$ *under* $+$
- $\mathbb{Q} - \{0\}$ *under* $\times$
- $GL(n, \mathbb{R})$ *under matrix multiplication (for invertible matrices only)*
- *the set of points on* $y^2 = x^3 + ax + b$ *over* $\mathbb{Q}$ *under point addition*
- *integer multiplication modulo* p *where* p *is prime.*
- $\mathbb{Z}_m$ *under the operation* $+$ *modulo* m $(\mathbb{Z}_m = \{0, 1, \ldots m - 1\})$
- $\mathbb{Z}_m^*$ *under the operation* $\times$ *modulo* m $(\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m | (x, m) = 1\})$.

Definition 2.9 *$Z(G)$ is the subset of elements of G that commute with every element of G.*

To be able to talk about the cardinality of a set in a group, we define the order of a group, G.

Definition 2.10 *The order of a finite group G, denoted $|G|$ is the number of elements in G.*

In the setting of a group, we often wish to do standard arithmetic. The structure often plays a role in this. To work with inverses, for instance, we take advantage of the following definition.

Definition 2.11 *Suppose G is a group and $a \in G$. We define $\frac{1}{a} = a^{-1} = b \in G$ where $a \bigoplus b = I \in G$.*

We can now do modular arithmetic with fractions:

Example 2 *Evaluate* $5/4 \pmod 7$. *Multiplication modulo 7 is a group. Further* 5 *and* $1/4 = 4^{-1}$ *are both elements of* G. *Now, since* $4^{-1} \equiv 2 \pmod 7$, *we simply compute:*

$$(5)(1/4) \equiv (5)(2) \equiv 10 \equiv 3 \pmod 7.$$

Among the most important types of groups is the set of cyclic groups. Cyclic groups play a special role in different aspects of number theory and cryptography. For examples see Koblitz [25] or Gallian [19].

Definition 2.12 *A finite group* G *which can be formed by computing powers of an element,* $g \in G$ *is called cyclic. In this case,* $G = \{e, g, g^2, g^3, \ldots, g^{k-1}\}$. *The element* g *is called the generator of the group. This group is often denoted by* $\langle g \rangle$.

Another important and richer algebraic structure that we will make use of is called a field.

Definition 2.13 *Let* $\mathbb{F}$ *be a set (with at least 2 elements) with operations* $+$ *and* $\times$ *defined on* $\mathbb{F}$ *satisfying the following three properties:*

1. $\mathbb{F}$ *is an abelian group with respect to* $+$.
2. $\mathbb{F} - \{0\}$ (0 *denotes the additive identity*) *is an abelian group with respect to* $\times$.
3. *For* $a, b, c \in \mathbb{F}$, $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$.

Then, $(\mathbb{F}, +, \times)$ *is said to be a field.*

Example 3

- $\mathbb{Q}, \mathbb{R}$ *and* $\mathbb{C}$ *are all fields.*
- $\mathbb{Z}_p$ *is a field under modular addition and multiplication if* p *is prime.*

- $\mathbb{F}_{2^n}$ *(the set of polynomials with coefficients in* $\{0,1\}$*) with modular addition and multiplication on polynomials is a field. For example,*

$$\mathbb{F}_{2^8} = \left\{a_7x^7 + a_6x^6 + a_5x^5 + \cdots + a_1x + a_0 | a_i \in \mathbb{Z}_2\right\}.$$

Note also that addition in $\mathbb{F}_{2^n}$ *is bitwise XOR and inverses can be computed using the extended Euclidean algorithm (see section 2.4).*

2.3 Quadratic Residues

Quadratic residues are often the basis for the mathematics underlying cryptographic concepts, for instance the Rabin Williams cryptosystem, the Legendre cryptosystem, and the Legendre factorization method [25]. We include this section to provide a basis when discussing the theory of factoring and prime testing. Only results which are truly important for what follows are included here. Quadratic residue results such as definitions and basic results can be found in [22] or [38].

Definition 2.14 *Let* m *be any integer. We say that* a *is a quadratic residue modulo* m *if* $(a,m) = 1$ *and there exists some* x *such that* $x^2 \equiv a \pmod{m}$.

We denote the set of quadratic residues modulo m as QR_m.

Definition 2.15 *Let* m *be any integer, and suppose that* $(a,m) = 1$ *and that* $x^2 \not\equiv a \pmod{m}$*, for any* x*. Then, we say that* a *is a quadratic non-residue modulo* m.

We denote the set of quadratic non-residues modulo m as QN_m. Notice, $\mathbb{Z}_m^* = QR_m \cup QN_m$.

Example 4 *Select* $m = 7$*. Then* $QR_7 = \{1,2,4\}$ *and* $QN_7 = \{3,5,6\}$*. Clearly,* $\mathbb{Z}_7^* = QR_7 \cup QN_7 = \{1,2,4\} \cup \{3,5,6\} = \{1,2,3,4,5,6\}$.

We shall see in subsequent chapters how quadratic residues can be used in prime tests and pseudo-prime tests. For instance, Euler's criterion provides an example of how one might implement quadratic residues to determine primality [41].

Theorem 2.6 (Euler's Criterion) *$a \in QR_p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Definition 2.16 *Let p be prime. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \in QR_p \\ -1 & \text{if } a \in QN_p \end{cases}.$$

It follows from Euler's criterion (Theorem 2.6) that, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Theorem 2.7 *The following properties hold for the Legendre symbol:*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \iff a \equiv b \pmod{p}$
4. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
5. $\left(\frac{t^2}{p}\right) = 1$ *if* $p \nmid t$
6. $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ *(Law of Quadratic Reciprocity).*

Example 5 *Evaluate* $\left(\frac{319}{1031}\right)$.

We could calculate $319^{\frac{1031-1}{2}} \pmod{1031}$*; however, this is computationally more difficult. Quadratic reciprocity yields a much simpler method.*

$$\begin{aligned}
\left(\frac{319}{1031}\right) &= \left(\frac{11 \cdot 29}{1031}\right) \\
&= \left(\frac{11}{1031}\right)\left(\frac{29}{1031}\right) && \textit{Property 2} \\
&= -\left(\frac{1031}{11}\right)\left(\frac{1031}{29}\right) && \textit{Property 6} \\
&= -\left(\frac{8}{11}\right)\left(\frac{16}{29}\right) && \textit{Property 3} \\
&= -\left(\frac{2}{11}\right) && \textit{Property 5 and 2} \\
&= 1. && \textit{Property 4}
\end{aligned}$$

Due to the restrictive nature of the Legendre symbol (i.e. the requirement of p to be prime), we introduce a more general version of the Legendre symbol called the Jacobi symbol [38].

Definition 2.17 *Let* $Q = \prod q_i^{\alpha_i}$ *be an odd integer. For any positive integer* P*, the Jacobi symbol* $\left(\frac{P}{Q}\right)$ *is defined by*

$$\left(\frac{P}{Q}\right) = \prod \left(\frac{P}{q_i}\right)^{\alpha_i},$$

where $\left(\frac{P}{q_i}\right)$ *is the Legendre symbol.*

Theorem 2.8 *The following properties hold for the Jacobi symbol:*

1. $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$
2. $\left(\frac{P_1}{Q}\right)\left(\frac{P_2}{Q}\right) = \left(\frac{P_1 P_2}{Q}\right)$
3. $P_1 \equiv P_2 \pmod{Q} \Longrightarrow \left(\frac{P_1}{Q}\right) = \left(\frac{P_2}{Q}\right)$

4. $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$

5. $\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}} \left(\frac{P}{Q}\right)$.

We now turn our attention to some of the fundamental algorithms in computational number theory.

2.4 Algorithms

Recall from Section 2.1 (Theorem 2.3 and its corollary) that the linear Diophantine equation

$$ax + by = 1$$

has no solution unless $(a, b) = 1$. The following algorithms allow us to solve for x and y and determine if $(a, b) = 1$. They can be found in more detail in Bressoud and Wagon [11].

Algorithm 2.1 (Euclidean Algorithm) *Let $\lfloor x \rfloor$ (the floor function) be the largest integer $\leq x$. Given $a, b \in \mathbb{Z}$ and $b > 0$,*

$$\begin{aligned}
a &= bq_0 + r_0 & q_0 &= \lfloor a/b \rfloor & 0 < r_0 < b \\
b &= r_0q_1 + r_1 & q_1 &= \lfloor b/r_0 \rfloor & 0 < r_1 < r_0 \\
r_0 &= r_1q_2 + r_2 & q_2 &= \lfloor r_0/r_1 \rfloor & 0 < r_2 < r_1 \\
&\vdots & &\vdots & \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} & r_{n-1} &= (a, b) & \\
r_{n-2} &= r_{n-1}q_n + r_n & r_n &= 0 &
\end{aligned}$$

Note that the Euclidean Algorithm determines whether on not $(a, b) = 1$. Further, $n < 5\log_{10}(\min\{a, b\}) = O(\log_{10}(\min\{a, b\}))$.

Algorithm 2.2 (Extended Euclidean Algorithm) *Let* $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$ *and define*

$$A_k = q_k A_{k-1} + A_{k-2}$$

$$B_k = q_k B_{k-1} + B_{k-2}$$

for $k = 0, 1, \ldots$ *and* q_i *as above. Then, a solution to the equation* $ax + by = 1$ *with* n *as in the Euclidean Algorithm, is given by*

$$x = (-1)^{n-1} B_{n-1}, \quad \text{and } y = (-1)^n A_{n-1}.$$

Another algorithm which is useful in computational number theory is known as Horner's Algorithm. Horner's algorithm (sometimes called the power algorithm) evaluates $a^n \pmod m$ given a, n, m.

Algorithm 2.3 (Horner's Method) *Given* a, n, m, *let* $n = b_0 2^k + b_1 2^{k-1} + \cdots + b_{k-1} 2 + b_k$ *be the binary expansion of* n *(*$b_0 = 1, b_i \in \{0, 1\}$*). Note that* $k = \lfloor \log_2 n \rfloor$. *Notice that we can evaluate* n *in the following way:*

$$2(\cdots(2(2b_0 + b_1) + b_2)\cdots + b_{k-1}) + b_k.$$

Now, Horner's method works as follows: put

$$s_0 = b_0$$

$$s_{i+1} = 2s_i + b_i \qquad i = 0, 1, \ldots k-1$$

to produce

$$s_k = n.$$

Now, define $r_i \equiv a^{s_i} \pmod m$ *for all* $i = 0, 1, \ldots, k$ *(where* r_i *is the least positive residue of* a^{s_i} *modulo* m*). Then*

$$r_k \equiv a^{s_k} \equiv a^n \pmod m.$$

Further, we can compute each r_i iteratively as follows:

$$r_{i+1} \equiv a^{s_{i+1}} \equiv a^{2s_i+b_{i+1}} \equiv (a^{s_i})^2 a^{b_{i+1}} \equiv (r_i)^2 a^{b_{i+1}} \pmod{m}$$

$$\equiv \begin{cases} r_i^2 \pmod{m} & \text{if } b_{i+1} = 0 \\ r_i^2 a \pmod{m} & \text{if } b_{i+1} = 1 \end{cases}.$$

This algorithm permits computation of a^n in $O(\log(2n))$ operations and uses no operands larger than m^2 (due to the modular arithmetic at every step).

Given a system of congruences

$$\begin{aligned} N &\equiv a_1 \pmod{p_1} \\ N &\equiv a_2 \pmod{p_2} \\ &\vdots \\ N &\equiv a_k \pmod{p_k}, \end{aligned}$$

one might wish to find a solution to this system in integers. One way to do this is with a theorem known as the Chinese Remainder Theorem [39].

Algorithm 2.4 (Chinese Remainder Theorem) *Let $\{p_1, p_2, \ldots p_k\}$ be distinct primes. Then, the following system of equations:*

$$\begin{aligned} N &\equiv a_1 \pmod{p_1} \\ N &\equiv a_2 \pmod{p_2} \\ &\vdots \\ N &\equiv a_k \pmod{p_k} \end{aligned}$$

has a unique solution for N modulo $\prod_{i=1}^{k} p_i$.

The Chinese Remainder Theorem (CRT) still holds if the p_i's are not prime provided that for all i and j, $(p_i, p_j) = 1$. Methods of recovering the solution to the system exist [38].

2.5 Bernoulli Numbers

Bernoulli numbers were first studied by Jakob Bernoulli (1654-1705) in the late 1600's and early 1700's while studying sums of powers of consecutive integers. Results regarding Bernoulli numbers were first published in 1713 in the posthumous work "Ars Conjectandi".

Currently, Bernoulli numbers are being studied in many different areas of mathematics such as number theory (including, but not limited to, distribution of primes and Fermat's last theorem), calculus of finite differences, combinatorics, Euler and Stirling sequences, Pascal's triangle, and differential topology.

The most modern definition of Bernoulli numbers is obtained through the generating function

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!} \qquad |t| < 2\pi. \tag{2}$$

This definition defines the n^{th} Bernoulli polynomial. Evaluating this polynomial at $x = 0$ yields the n^{th} Bernoulli number. This function and other results can be found in Abramowitz and Stegun's book The Handbook of Mathematical Functions [1].

Perhaps a more convenient definition of Bernoulli numbers is obtained by the following recursive definition [1]:

Definition 2.18 *Take $B_0 = 1$. Then the n^{th} Bernoulli number is:*

$$B_n = \frac{1}{n+1}\sum_{i=0}^{n-1}\binom{n+1}{i}B_i. \tag{3}$$

It is not hard to show that Definition 2.18 follows from the generating function in equation (2). We will take equation (3) as the definition of a Bernoulli number instead of the more general definition given by equation (2).

$B_0 =$	1	$B_1 =$	$\frac{-1}{2}$
$B_2 =$	$\frac{1}{6}$	$B_3 =$	0
$B_4 =$	$\frac{-1}{30}$	$B_5 =$	0
$B_6 =$	$\frac{1}{42}$	$B_7 =$	0
$B_8 =$	$\frac{-1}{30}$	$B_9 =$	0
$B_{10} =$	$\frac{5}{66}$	$B_{11} =$	0
$B_{12} =$	$\frac{-691}{2730}$	$B_{13} =$	0
$B_{14} =$	$\frac{7}{6}$	$B_{15} =$	0

Table 1: The First 15 Bernoulli Numbers

Each Bernoulli number with an odd index greater than 1 is zero. This is an easy consequence of Definition 2.18 and the symmetry given by the Binomial Theorem [1]. Further, one can show the following generalization of Definition 2.18 [1].

Lemma 2.3

$$B_n(x+h) = \sum_{k=0}^{n} \binom{nk}{B}_k (x)h^{n-k} \qquad n \in \mathbb{N}.$$

The following theorem is due to Raabe [46]. It plays a significant role in the study of Bernoulli polynomials.

Theorem 2.9 (Raabe) *Let $m > 0$ and $n \geq 0$ be integers. Then*

$$\sum_{r=0}^{m-1} B_n\left(\frac{x+r}{m}\right) = m^{1-n}B_n(x).$$

The next lemma [46], outlines the relationship between Bernoulli numbers and sums of powers of consecutive integers.

Lemma 2.4

$$\sum_{k=1}^{m} k^n = \frac{B_{n+1}(m+1) - B_{n+1}}{n+1} \quad \forall\, m, n \in \mathbb{Z}^+.$$

Table 2 provides some well known bounds on the magnitude of Bernoulli numbers.

$\lvert B_{2n}\rvert > \lvert B_{2n}(x)\rvert$	$n = 1, 2, \ldots$	$0 < x < 1$
$\frac{2(2n+1)!}{(2\pi)^{2n+1}} \frac{1}{1-2^{-2n}} > (-1)^{n+1} B_{2n+1}(x) > 0$	$n = 1, 2, \ldots$	$0 < x < \frac{1}{2}$
$\frac{2(2n)!}{(2\pi)^{2n}} \frac{1}{1-2^{1-2n}} > (-1)^{n+1} B_{2n} > \frac{2(2n)!}{(2\pi)^{2n}}$	$n = 1, 2, \ldots$	

Table 2: Inequalities Related to Bernoulli Numbers [46]

The structure of Bernoulli numbers remains largely unknown. There are methods of calculating Bernoulli numbers without using the generating function or the recursive definition. These methods often require approximating the Zeta function and calculating the numerator of the Bernoulli number based on a known denominator. Results involving approximating the Zeta function will be discussed in Section 2.11. One result regarding the structure of Bernoulli number denominators (where each B_n is assumed to be in lowest terms), denoted $denom(B_n)$, is a result of von Staudt and Clausen [35].

Theorem 2.10 (von Staudt - Clausen Theorem) *Let B_{2n} be the $2n^{th}$ Bernoulli number. Then, $p - 1 \mid 2n$, if and only if $p \mid denom(B_{2n})$.*

Corollary 2.2 *$B_{2n} = A_{2n} - \sum_{p-1|2n} \frac{1}{p}$, where $A_{2n} \in \mathbb{Z}$.*

Even though von Staudt and Clausen's theorem gives no information about the numerator of Bernoulli numbers, the denominators are determined simply through finding integers p such that $(p-1)|2n$.

2.6 Bernoulli Numbers Modulo p

Among the most important properties of Bernoulli numbers is the so-called Kummer congruence. Kummer's 1850 result is one of fundamental importance to this thesis and to number theory as a whole. Kummer's congruence relates Bernoulli numbers whose indices are in the same residue class modulo $p-1$, modulo a prime, p [35].

Theorem 2.11 (Kummer's Congruence) *Let $k \in \mathbb{N}$, $p \in \mathbb{P}$ and $b \not\equiv 0 \pmod{p-1}$. Then the following equivalence holds*

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \frac{B_b}{b} \pmod{p}.$$

Much work has been done to generalize Kummer's result from a modulo p result to a modulo p^k result. We list some known results in Table 3.

For $k \in \mathbb{N}$, Kummer's congruence implies a first order relationship between $B_{k(p-1)+b}$ and B_b of the form

$$B_{k(p-1)+b} \equiv B_b + mk \pmod{p}$$

whenever $(k(p-1)+b)^{-1}$ exists modulo p. To see this, multiply both sides of Kummer's congruence by $k(p-1)+b$ and observe the following congruences:

$$B_{k(p-1)+b} \equiv (k(p-1)+b)\frac{B_b}{b} \pmod{p} \tag{4}$$

$$\equiv B_b + \frac{k(p-1)}{b}B_b \pmod{p}. \tag{5}$$

Now, suppose that

$$B_b + \frac{k(p-1)}{b}B_b \equiv B_b + mk \pmod{p}, \tag{6}$$

for some constant $m \in \mathbb{Z}$, and $b \not\equiv 0 \pmod{p-1}$. After subtracting B_b from both sides, equation 6 implies that

$$\frac{kp}{b}B_b - \frac{k}{b}B_b \equiv mk \pmod{p}. \tag{7}$$

Congruence	Reference
$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \frac{B_b}{b} \pmod{p} \; \forall \; k \in \mathbb{N}$	Kummer [35]
$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv k\frac{B_{p-1+b}}{p-1+b} - (k-1)(1-p^{b-1})\frac{B_b}{b} \pmod{p^2}$	Sun [42]
$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv$ $\binom{k}{2}\frac{B_{2(p-1)+b}}{2(p-1)+b} - k(k-2)\frac{B_{p-1+b}}{p-1+b} + \binom{k-1}{2}(1-p^{b-1})\frac{B_b}{b} \pmod{p^3}$	Sun [42]
$B_{p-3} \equiv \frac{-3}{p^2}(\sum_{i=1}^{n-1}\frac{1}{i})$	Sun [42]
$(p-1)! \equiv \frac{pB_{2p-2}}{2p-2} - \frac{pB_{p-1}}{p-1} - \frac{1}{2}(\frac{pB_{p-1}}{p-1})^2 \pmod{p^3}$	Sun [42]
For $b > n$ and $b \not\equiv 0 \pmod{p-1}$ $\sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv 0 \pmod{p^n}$	Ireland and Rosen [22]
$\frac{B_k(x)-B_k(x_0)}{k} \equiv (x-x_0)B_{k-1} \pmod{p}$	Sun [42]
$(1-p^{k(p-1)+b-1})\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}$ $(1-p^{r(p-1)+b-1})\frac{B_{r(p-1)+b}}{r(p-1)+b} \pmod{p^n}$	Sun [42]
For $k \in \{1,2,\ldots,p-4\}$, $\sum_{x=1}^{p-1}x^{-k} \equiv \begin{cases} \frac{k(k-1)}{2}\frac{B_{p-2-k}}{p-2-k}p^2 \pmod{p^3} & \text{if } k \text{ is odd} \\ k(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k})p \pmod{p^3} & \text{if } k \text{ is odd} \end{cases}$	Sun [42]
$\sum_{x=1}^{p-1}x^{-(p-3)} \equiv (\frac{1}{2} - 3B_{p+1})p - \frac{4}{3}p^2 \pmod{p^3}$	Sun [42]
$\sum_{x=1}^{p-1}x^{-(p-2)} \equiv -(2-pB_{p-1})p - \frac{5}{2}p^2 \pmod{p^3}$	Sun [42]
$\sum_{x=1}^{p-1}x^{-(p-1)} \equiv pB_{2p-2} - 3pB_{p-1} + 3(p-1) \pmod{p^3}$	Sun [42]
For $k < p$ then, $\sum_{x=1}^{p-1}x^{-1} \equiv \begin{cases} \frac{k}{k+1}pB_{p-1-k} \pmod{p^2} & \text{if } k < p-1 \\ -pB_{p-1} + 2(p-1) \pmod{p^2} & \text{if } k = p-1 \end{cases}$	Sun [42]
For $p > 3$, then $\frac{\sum_{r=0}^{p-1}r^k - pB_k}{k} \equiv \frac{p}{2}pB_{k-1} \pmod{p^2}$	Sun [43]
For $p > 3$, then $(p-1)! \equiv pB_{p-1} - p \pmod{p^2}$	Beeger [7]

Table 3: Congruences Involving Bernoulli Numbers

Dividing k from both sides, and assuming $\frac{1}{b}B_b$ is invertible modulo p (i.e. the denominator has a multiplicative inverse in $\mathbb{Z}_p$), then

$$-\frac{B_b}{b} \equiv m \pmod{p}. \tag{8}$$

Therefore, the linear relationship between $B_{k(p-1)+b}$ and B_b is

$$B_{k(p-1)+b} \equiv B_b - \frac{B_b}{b} \pmod{p}$$

with $-\frac{B_b}{b}$ constant. Higher order relationships may be derived modulo p^α; however, relationships of this form become increasingly complex as α increases.

2.7 Euler Numbers

Closely related to Bernoulli numbers are the Euler numbers. All results in this section can be found in The Handbook of Mathematical Functions [1]. Euler polynomials are generated by the following function, similar to the generating function for Bernoulli polynomials:

$$\frac{2e^{xt}}{e^t+1} = \sum_{n=0}^{\infty} E_n(x)\frac{t^n}{n!} \qquad |t| < \pi. \tag{9}$$

$E_n(x)$ is known as the Euler polynomial. The numerator of the value of polynomial after being evaluated at $x = \frac{1}{2}$, yields the value of the n^{th} Euler number, E_n. In fact, the denominator of the evaluated polynomial is 2^n so,

$$E_n = 2^n E_n(1/2).$$

As with Bernoulli numbers, there is a recursive formula which may be used to describe Euler polynomials.

Lemma 2.5 *The n^{th} Euler polynomial satisfies*

$$E_n(x+h) = \sum_{k=0}^{n} \binom{n}{k} E_k(x)h^{n-k} \quad n \in \mathbb{N},\ h \in \mathbb{Z}^+,\ x \in \mathbb{R}. \tag{10}$$

Clearly, $x + h = \frac{1}{2}$ is a simple point at which to evaluate as $x = -1/2$, $h = 1$ will yield a simple solution. It is also important to note that $E_n(0) = -E_n(1)$. Hence, Euler numbers can be given as a function of the constant term of Euler polynomials with smaller indices.

The definition given in equation (9) is equivalent to that in Lemma 2.5. It can also be shown that any Euler number with odd index is zero. Further, one can show that the signs of the even indexed Euler numbers alternate as depicted in Table 4.

$E_0 =$	1	$E_1 =$	0
$E_2 =$	-1	$E_3 =$	0
$E_4 =$	5	$E_5 =$	0
$E_6 =$	-61	$E_7 =$	0
$E_8 =$	1385	$E_9 =$	0
$E_{10} =$	-50521	$E_{11} =$	0
$E_{12} =$	2702765	$E_{13} =$	0

Table 4: The First 13 Euler Numbers

The next lemma is a useful characterization of Euler polynomials.

Lemma 2.6

$$E_n(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{E_k}{2^k} \left(x - \frac{1}{2}\right)^{n-k}. \tag{11}$$

Much like Bernoulli polynomials, Euler polynomials can be characterized in terms of sums of powers of integers.

Lemma 2.7

$$\sum_{k=1}^{m} (-1)^{m-k} k^n = \frac{E_n(m+1) + (-1)^m E_n(0)}{2} \quad m, n \in \mathbb{N} \tag{12}$$

We conclude this section with some important relationships between Bernoulli numbers and Euler polynomials.

Lemma 2.8

$$E_{n-1}(x) = \frac{2}{n}\left\{B_n(x) - 2^n B_n\left(\frac{x}{2}\right)\right\} \tag{13}$$

$$E_{n-1}(x) = \frac{2^n}{n}\left\{B_n\left(\frac{x+1}{2}\right) - B_n\left(\frac{x}{2}\right)\right\} \tag{14}$$

$$E_n(0) = -E_n(1) = -2(n+1)^{-1}(2^{n+1} - 1)B_{n+1} \tag{15}$$

2.8 The Riemann Zeta Function

The Riemann zeta function is among the most important special functions in mathematics and physics. The Zeta function can be found in the study of prime number theory, lattice theory, probability, distribution of primes, complex contour integration, and in areas of physics such as entropy, and statistical mechanics. There are many hypothesized properties of the Zeta function that remain unproved. The most notable of these results is the so called Riemann Hypothesis [53]. We will be interested in the characterization of the Zeta function as it relates to sums of reciprocal powers.

The Zeta function is defined in the following way [1]:

Definition 2.19 *When $\mathcal{R}[n] > 1$ (where $\mathcal{R}[n]$ is the real part of n), Riemann's Zeta function is defined as follows:*

$$\zeta(n) = \sum_{k=1}^{\infty} \frac{1}{k^n}.$$

This definition is equivalent to saying that

$$\zeta(n) = \prod_{p \in \mathbb{P}} (1 - p^{-n})^{-1},$$

where again $\mathcal{R}[n] > 1$.

The Zeta function can also be defined by the following sum [53]:

$$\zeta(n) = \frac{1}{n-1} + \sum_{s=0}^{\infty} \frac{(-1)^s}{s!} \gamma_s (n-1)^s,$$

where

$$\gamma_n = \lim_{m \to \infty} \left\{ \sum_{k=1}^{m} \frac{(\ln(k))^n}{k} - \frac{(\ln(m))^{n+1}}{n+1} \right\} \quad \text{with } \mathcal{R}(n) > 0.$$

is called the Stieltjes constant.

As defined above, $\zeta(n)$ is a complex number with $\mathcal{R}[n] > 1$. The Zeta function, however, has a unique analytic continuation to all of the complex plane with the exception of a simple pole at $n = 1$.

$\zeta(0) =$	$-\frac{1}{2}$	$\zeta(-1) =$	$-\frac{1}{2}$
$\zeta(1) =$	undefined	$\zeta(-2) =$	0
$\zeta(2) =$	$\frac{1}{6}\pi^2$	$\zeta(-3) =$	$\frac{1}{120}$
$\zeta(3) \simeq$	1.202	$\zeta(-4) =$	0
$\zeta(4) =$	$\frac{1}{90}\pi^4$	$\zeta(-5) =$	$-\frac{1}{252}$
$\zeta(5) \simeq$	1.036	$\zeta(-6) =$	0
$\zeta(6) =$	$\frac{1}{945}\pi^6$	$\zeta(-7) =$	$\frac{1}{240}$
$\zeta(7) \simeq$	1.008	$\zeta(-8) =$	0

Table 5: Values of the Riemann Zeta function

For n even and negative, $\zeta(n) = 0$. These roots are referred to, in the literature, as trivial zeros. All non-trivial zeros occur for $n = \sigma + it$ when $0 \leq \sigma \leq 1$. The

Riemann hypothesis asserts that all non trivial zeros have the form $n = \frac{1}{2} + it$ [53]. For n even and positive, $\zeta(n) = \frac{l\pi^n}{k}$ for some integers k and l as seen in Table 5.

The following result shows a connection between the Zeta function and contour integrals.

Theorem 2.12

$$\zeta(n) = -\frac{\Gamma(1-n)}{2\pi i} \oint_\gamma \frac{(-z)^{n-1}}{e^z - 1} dz$$

where γ is the contour in figure 1, and Γ is the gamma function defined by:

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \quad \text{with } \mathcal{R}(z) > 0$$

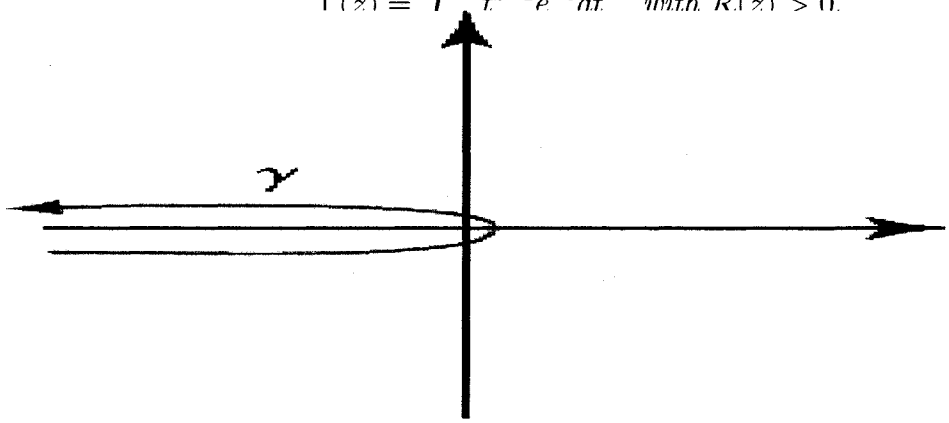

Figure 1: Contour for Riemann's Zeta function [53].

Table 6 highlights some relations between the Zeta function and Bernoulli numbers.

2.9 Prime Tests

Primality proving is a rapidly changing area of number theory. With this in mind, I have made little effort to provide a complete historical overview, nor has much effort been made to provide more than a couple of modern prime tests (and not in much detail). This section should provide no more than a starting point for a more detailed study.

Relation	Condition
$\zeta(n) = \frac{1}{n-1} + \frac{1}{2} + \sum_{k=1}^{n} \frac{B_{2k}}{2k} \binom{n+2k-2}{2k-1} - \binom{n+2s}{2s+1} \int_1^\infty \frac{B_{2s+1}(x-[x])}{x^{n+2s+1}} dx$	$n \neq 1$ $s \in \mathbb{Z}^+$ $\mathcal{R}(n) > -2s$
$\zeta(2n+1) = \frac{(-1)^{n+1}(2\pi)^{2n+1}}{2(2n+1)!} \int_0^1 B_{2n+1}(x) \cot(\pi x) dx$	$n \in \mathbb{Z}^+$
$\zeta(1-2n) = -\frac{B_{2n}}{2n}$	$n \in \mathbb{Z}^+$
$\zeta(2n) = \frac{(2\pi)^{2n}}{2(2n)!} \lvert B_{2n} \rvert$	$n \in \mathbb{Z}^+$

Table 6: Relations Between the Riemann Zeta Function and Bernoulli Numbers [1].

Definition 2.20 *A prime number is a positive integer $p > 1$, with exactly two positive divisors, 1 and itself. A positive integer, larger than 1, which is not prime is said to be composite. A prime test is any test which certifies a number to be prime or composite.*

There are two main types of prime tests: deterministic and probabilistic. Deterministic tests determine primality with 100% certainty while probabilistic tests potentially identify composite numbers as prime (albeit with small probability).

Historically, the most primitive deterministic prime test is the method of trial division. This method involves dividing n by each integer less than $\sqrt{n}$.

Wilson's theorem yields another deterministic primality test:

$$n \text{ is prime } \Leftrightarrow (n-1)! \equiv -1 \pmod{n}.$$

Both Wilson's theorem and trial division are far too slow to be of practical value.

The most commonly used probabilistic prime test is given by Fermat's Little Theorem (Theorem 2.5)

$$n \text{ is prime } \Longrightarrow a^{n-1} \equiv 1 \pmod{n} \ \forall\, 1 < a < n.$$

The converse of this theorem, given a randomly chosen a with $(a, n) = 1$,

$$a^{n-1} \equiv 1 \pmod{n},$$

implies that n is prime with probability $1 - \frac{1}{2^k}$, where k is the number of trials. Of course Carmichael numbers (which will be discussed in detail later) always satisfy this equation (and Carmichael numbers are always composite). Because of Carmichael numbers, Fermat's Little Theorem is only a probabilistic test.

In August 2002, three Indian mathematicians Agrawal, Kayal, and Saxena submitted the first deterministic polynomial-time algorithm to determine primality. Their algorithm relies on the following lemma [4].

Lemma 2.9 *Suppose that* $(a, p) = 1$. *Then* p *is prime if and only if*

$$(x - a)^p \equiv (x^p - 1) \pmod{p}.$$

The AKS test (as it is known) is both unconditional and non-randomized. That is, it does not rely on conjectural results (i.e. the Riemann Hypothesis) or on choosing numbers carefully or randomly. The algorithm runs as follows:

Algorithm 2.5 (AKS Algorithm) *Input* $n > 1$.

1. if (n is of the form a^b, $b > 1$*) output COMPOSITE;*

2. $r = 2$;

3. while $(r < n)$ {

4. if ($(n, r) \neq 1$ *) output COMPOSITE;*

5. *if (r is prime)*

6. *let q be the largest prime factor of* $r-1$*;*

7. *if (* $q \geq 4\sqrt{r}\log n$ *) and (*$n^{\frac{(r-1)}{q}} \not\equiv 1 \pmod{r}$*)*

8. *break;*

9. $r \leftarrow r+1$*;*

10. }

11.

12. for $a = 1$ *to* $2\sqrt{r}\log n$

13. *if (* $(x-a)^n \not\equiv (x^n - a) \pmod{x^r - 1, n}$*) output COMPOSITE;*

14. output PRIME;

The runtime of the algorithm in the original paper was $O((ln\ n)^{12})$. Current implementations run in $O((ln\ n)^6)$ for general integers [32].

The elliptic curve prime proving method was motivated by new results in the theory of elliptic curves. Since entire courses are devoted to the study of elliptic curves, a simple framework will be provided here for the reader to begin individual study.

Theorem 2.13 *Let* N *be an integer co-prime to 6,* E *an elliptic curve over* $\mathbb{Z}_N$*, together with a point* P *on* E *and* m *and* s *two integers with* $s|m$*. For each prime divisor* q *of* s*, put* $(\frac{m}{q})P = (x_q : y_q : z_q)$*, the residue class of* (x, y, z)*. Assume that* $mP = O_E$ *is the point at infinity and* $\gcd(z_q, N) = 1$ *for every* q*. Then, if* p *is a prime divisor of* N*, one has* $\#E(Z_p) \equiv 0 \pmod{s}$*, where* $\#E(Z_p)$ *represents the number of integral points on the elliptic curve,* E*.*

This result provides a basis for the Goldwasser-Kilian algorithm.

Algorithm 2.6 (Goldwasser-Kilian) *Input* $n > 1$.

1. Choose an elliptic curve E *over* $\mathbb{Z}_n$ *for which the number of points* m *satisfies* $m = 2q$ *where* q *is a probable prime;*

2. If (E, m) *satisfies the conditions of Theorem 2.13 with* $s = m$*, then* n *is prime, otherwise it is composite;*

3. The primality of q *is proved in the same way;*

4. Output results.

The Goldwasser-Kilian algorithm proves the primality of n in expected time of $O((\log n)^{10+c})$, where c is a constant independent of n. Improvements have been made to this algorithm; however, without sufficient background in elliptic curves a statement of the algorithm seems rather fruitless The improved algorithm (known as ECPP) has a run time of roughly $O((\log n)^{6+\varepsilon})$ for some $\varepsilon > 0$.

2.10 Factoring Algorithms

Tests which certify that a number, n, is composite often give no indication of the divisors of n. A factoring algorithm yields a factor (prime or not) or a series of factors of n. A good reference for further study on factoring algorithms and a book in which most recent results are stated is Koblitz [25].

Historically, the method of direct search factorization (essentially trial division) was the first and arguably the least sophisticated method of factoring. Requiring at most $\sqrt{n}$ trial divisions, direct search factoring is essentially only a preliminary tool used before more sophisticated algorithms.

Modern factoring algorithms take advantage of many different branches of number theory. For example, the elliptic curve factoring algorithm takes advantage of the theory of elliptic curves, the quadratic sieve takes advantage of Dixon's algorithm

and factoring differences of squares, and the number field sieve uses similar ideas to the quadratic sieve while taking advantage of polynomials which are not quadratic.

The elliptic curve factoring method starts with selecting an elliptic curve E in "short Weierstrass form" (that is, a curve of the form

$$y^2 = x^3 + ax + b \tag{16}$$

with $4a^3 + 27b^2 \neq 0$) over the field $\mathbb{Z}_n^*$. Notice that if p is a prime divisor of n, and $a \equiv b \pmod{n}$, then necessarily $a \equiv b \pmod{p}$. This property always holds for points on elliptic curves with the exception of division (i.e. if a or b is a fraction which is invertible modulo p, it need not be invertible modulo n). To compute $a/b \pmod{n}$, b must be invertible modulo n. If b is invertible modulo p, it need not be invertible modulo n.

In general, computing points on an elliptic curve is a straightforward calculation. Algebraically, for $P = (x_P, y_P)$, and $Q = (x_Q, y_Q)$, $P + Q = R = (x_R, y_R)$ where

$$x_R = s^2 - x_P - x_Q, \text{ and } y_R = -y_P + s(x_P - x_R),$$

$$s = \frac{y_P - y_Q}{x_P - x_Q}.$$

Here, s represents the slope of the line through P and Q. Notice that point addition in the context of elliptic curves is not componentwise. To compute $2P$ algebraically, find

$$s = \frac{3x_P^2 + a}{2y_P},$$

which gives values

$$x_R = s^2 - 2x_P, \quad \text{and} \quad y_R = -y_P.$$

Clearly, $3P = 2P + P$, etc.

To factor n, select a point P satisfying equation (16) and compute $Q = RP$ where R is a large positive integer divisible by all prime powers less than some bound B. Clearly, $Q = RP$ can easily be computed unless there is a division by zero; however, in this case, a factor of n is found (the greatest common divisor of n and the denominator). If that factor is n itself or if Q is successfully computed, repeat the process as we have failed to find a factor of n.

The elliptic curve method for factoring factors in expected time [12]

$$\exp((0.5 + o(1))(\log n)^{1.414}(\log\log n)^{0.5}).$$

Similarly, the quadratic sieve factors a number n in expected time [12]

$$\exp((0.5 + o(1))(\log n)^{1.02}(\log\log n)^{0.5}).$$

The quadratic sieve, unlike the elliptic curve method, requires a factor base $F = \{p_1, \ldots p_m\}$. Essentially, the quadratic sieve is a factorization method which relies on finding two integers x and y for which

$$x^2 \equiv y^2 \pmod{n} \quad \text{but} \quad x \not\equiv y \pmod{n},$$

using the factor base F. If such a situation arises, it is known that either $(x - y, n)$ or $(x + y, n)$ is a non-trivial factor of n with high probability. What is required to find x and y is to construct a sequence of positive integers r_i for which

$$f(r_i) \equiv r^2 - n \pmod{n}.$$

Let U be the set of these r_i. When more than m of these r_i terms are found, we have

$$\prod_{r_i \in U} f(r_i) = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_m^{2\alpha_m} = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m})^2.$$

To form x and y, set

$$x = \prod_{r_i \in U} r_i \quad \text{and} \quad y = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}.$$

Therefore,

$$x^2 = \prod_{r_i \in U} r_i^2 \equiv \prod_{r_i \in U} (r_i^2 - n) \equiv \prod_{r_i \in U} f(r_i) \equiv y^2 \pmod{n}.$$

Finally, the Euclidean algorithm determines both $(x - y, n)$ and $(x + y, n)$.

As mentioned, the time complexity of both the elliptic curve method of factoring and the quadratic sieve are very similar. The multi-polynomial quadratic sieve (an improvement over the quadratic sieve) yields a heuristic expected time [12] of

$$\exp((1 + o(1))(\log n)^{0.5}(\log \log n)^{0.5}).$$

As the name suggests, the multi-polynomial quadratic sieve takes advantage of several polynomials of the form $f(x) = ax^2 + bx + c$ where a is a square, $0 \leq b < a$ such that $b^2 \equiv n \pmod{a}$ and $b^2 - 4ac = n$. With some arithmetic, it can be shown that

$$(ax + b)^2 \equiv af(x) \pmod{n},$$

and since a is a square, so too is $f(x)$. So, if $f(x)$ factors easily, we obtain a similar factoring situation to the quadratic sieve.

Finally, the number field sieve provides an even better expected time of approximately,

$$\exp((1.526 + o(1))(\log n)^{1/3}(\log \log n)^{2/3}).$$

Unlike previously mentioned algorithms, the number field sieve attempts to factor integers n of the form

$$n = r^e \pm s, \quad \text{where} \quad r, s \in \mathbb{Z}^+.$$

Unfortunately, due to the extensive amount of algebraic number theory required to fully appreciate the algorithm, a complete overview is not given here. However, the idea behind the sieve is that both the algebraic integer $a + b\alpha$ and the integer $a + bm$ are smooth over a factor base. If Φ is a ring homomorphism between $\mathbb{Z}[\alpha]$ and $\mathbb{Z}_n$, then

$$\Phi(a + b\alpha) = (a + bm \pmod{n}).$$

With sufficiently many of these congruences, one can find a solution to the equation

$$y^2 \equiv z^2 \pmod{n},$$

which in turn may yield a non-trivial factor of n.

2.11 Computing B_n and $\zeta(n)$

Much research has been done in computing both the Bernoulli number, B_n, and the value of the zeta function, $\zeta(n)$. Many of the techniques which are currently in use are described in the recent paper "Computational Strategies for the Riemann Zeta Function" [9].

Most computational work does not deal with the general problem of determining the value of $\zeta(n)$ or B_n for a general integer value of n. Indeed, the majority of the research seems to lie in two different areas: computing $\zeta(n)$ for a few select values of n (say $n = 3$ or 5) in an interesting way, and computing complex zeros of the zeta function. Neither of these themes seems overly useful in the context of this thesis as we are primarily interested in exact fractional values of B_n and values of the zeta function of the form $a\pi^k/b$. Nevertheless, a brief description of these methods is still in order.

Recall that for $n \in \mathbb{Z}^+$, $\zeta(1-2n) = \frac{-B_{2n}}{2n}$ and for $n \in \mathbb{Z}^+$, $\zeta(2n) = \frac{(2\pi)^{2n}}{2(2n)!}|B_{2n}|$.

Therefore, any computational technique used to compute values of the zeta function can also be used to compute Bernoulli numbers. With this in mind, we concentrate on algorithms to compute values of the zeta function.

Standard recurrence relations can be used to find the value of $\zeta(n)$. For instance, with $k \geq 2$,

$$\sum_{j=1}^{k-1} \zeta(2j)\zeta(2k-2j) = (k+\frac{1}{2})\zeta(2k).$$

Although this yields exact values for $\zeta(2k)$, it is rarely used as $k-1$ previous values of the zeta function must be a priori known.

To approximate values of the zeta function in the complex plane, one can use the formula

$$\zeta(s) = -\sum_{j=0}^{\infty} \frac{(-\pi i)^j}{j!}\eta(s-j),$$

where

$$\eta(s) = \frac{1}{\Gamma(s)}\int_0^{\infty} \frac{t^{s-1}}{e^t+1}dt$$

and Γ is the gamma function. This method is referred to as a "Lerch-series approach." The Lerch-series approach can be used whenever $s \in \mathbb{C}$ and $\mathcal{R}[s] > 0$.

Approximations to values of the zeta function for integers have become increasingly easy to obtain due to the current ease of approximating π. Of major interest, is the value of $\zeta(3)$. Many different formulations have been derived for $\zeta(3)$ with the hope of being able to simply extend the formulations to $\zeta(n)$ for arbitrary n. One example stems from the following equality [16]:

$$-\frac{(1-2^{-2m-1})2\zeta(2m+1)}{(\pi i)^{2m}} = \sum_{k=1}^{m-1} \frac{(1-4^{-k})\zeta(2k+1)}{(\pi i)^{2k}(2m-2k)!} + \frac{1}{(2m)!}\left\{\log 2 - \frac{1}{2m} + \sum_{n=1}^{\infty} \frac{\zeta(2n)}{4^n(n+m)}\right\}$$

which, for $m = 1$, yields

$$\zeta(3) = \frac{2\pi^2}{7}\left\{\log 2 - \frac{1}{2} + \sum_{n=1}^{\infty} \frac{\zeta(2n)}{4^n(n+1)}\right\}.$$

Of course, once one has $\zeta(3)$, computing $\zeta(5)$ is straightforward and once $\zeta(3)$ and $\zeta(5)$ are known, computing $\zeta(7)$ is straightforward etc. Notice also that the term $\frac{1}{(2m)!}\left\{\log 2 - \frac{1}{2m} + \sum_{n=1}^{\infty} \frac{\zeta(2n)}{4^n(n+m)}\right\}$ converges quickly because of the $(2m)!$ and 4^n terms in the denominator. Therefore, values of the zeta function for odd integers are easy to approximate. A similar formula holds for even integral inputs, however it is not as simple to compute. This approach is known as "recycling" as previous values of the zeta function are recycled while trying to compute a current value.

Another recycling approach is given by the following algorithm due to Crandall [16].

Algorithm 2.7 (Recycling Scheme for $\zeta(2), \ldots \zeta(L+1)$)

1. ***Set Precision***

   Select N such that 2^{-N} is less than the required precision and $N > L$.

2. ***Quotient Array***

   Create $g(k) = P(k)/Q(k)$, for $k \in [0, 4N-1]$, where $P(k) = (-N)^k$, and $Q(k) = k!(k+1-z)$.

3. ***Resolve g Function***

$p = 1$;

while $p \leq 2N$ *do*

for $q = 0$ *to* $4N - 1 - p$ *do*

$g(q) = g(q)+g(q+p)$ *with* $g(q)$ *in the form numerator/ denominator and reduced modulo* z^{L+1};

end;

$p = 2p$;

end;

4. ***Monic Reversion***

Now, $g(0) = P(0)/Q(0)$ *with each of* P, Q *being of degree at most* L, *so divide each of* P, Q *through by its constant coefficient;*

5. ***Inversion***

Create polynomials P^{-1} *and* Q^{-1} *using Newton inversions. For instance, to find* P^{-1},

set $p = g = 1$

while $(p < deg(P))$ *do*

$p = \max(2p, deg(P))$;

$h = P \pmod{z^p}$;

$g = (g + g \cdot (1 - h \cdot g)) \pmod{z^p}$

end;

6. ***Coefficient Computation***

Compute the coefficients R_k *in the polynomial*

$$R(z) = \sum_{k=0}^{L} R_k z^k = ((dP/dz)P^{-1} - (dQ/dz)Q^{-1}) \pmod{z^{L+1}}.$$

7. ***Output*** ζ ***Values***

$\zeta(k) \sim R_{k-1}$

The operation complexity of this algorithm is $O(L^{-1}N \log^2 L)$ for each of the L evaluations of ζ. So, if $L \sim N$, (that is D values with each to D digits) the average cost is about $O(\log^2 D)$ per value.

A third approach, due to Plouffe and Fee [16] uses the von Staudt-Clausen theorem to compute the denominator of B_n and asymptotic techniques to determine the numerator. The result is an exact value for B_n which can easily be converted to a value of ζ. The tricky part of this algorithm is determining the value of the denominator which is essentially a problem of factoring $n - 1$. This approach was used to determine the value B_{200000} in its rational form.

3 Giuga's Conjecture

In 1950, G. Giuga proposed the following [20]:

$$n \text{ is prime } \Leftrightarrow s(n) := \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}.$$

If n is prime, then by Fermat's Little Theorem, (Theorem 2.5)

$$\sum_{k=1}^{n-1} k^{n-1} \equiv \sum_{k=1}^{n-1} -1 \equiv n-1 \equiv -1 \pmod{n}.$$

Thus, the converse is all that remains as conjecture. We shall denote the set of positive integers $n \geq 2$ that satisfy $s(n) \equiv -1 \pmod{n}$ by Σ.

In this way, we see that $\mathbb{P} \subset \Sigma$ and Giuga's conjecture asserts that $\mathbb{P} = \Sigma$. In his original paper [20], Giuga proved that any composite integer $n \in \Sigma$ must satisfy $(p-1)|((n/p)-1)$ and $p|((n/p)-1)$, for every prime divisor p of n. We include the proof here for completeness [8].

Theorem 3.1 *$n \in \Sigma$ if and only if for each prime divisor p of n we have*

$$(p-1) \mid ((n/p)-1) \text{ and } p \mid ((n/p)-1).$$

Proof: Before directly proving the equivalence, a general property is established. Suppose that $(p-1)|(n-1)$. Then $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$ by Fermat's Little Theorem (Theorem 2.5). If $(p-1) \not| (n-1)$, then it must be true that $\sum_{k=1}^{n-1} k^{n-1} \equiv 0 \pmod{n}$ (Theorem 2.2). So, we have:

$$\sum_{k=1}^{p-1} k^{n-1} \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1)|(n-1) \\ 0 \pmod{p} & \text{otherwise} \end{cases}. \tag{17}$$

Therefore, for every prime divisor p of n, with $n = pq$, it must be the case, by considering residue classes, that :

$$\sum_{k=1}^{n-1} k^{n-1} \equiv q \sum_{k=1}^{p-1} k^{n-1} \equiv \begin{cases} -q \pmod{p} & \text{if } (p-1)|(n-1) \\ 0 \pmod{p} & \text{otherwise} \end{cases}, \tag{18}$$

as we are considering the class of $p-1$ q-times. This result is now employed in the direct proof.

($\Rightarrow$) Let $n \in \Sigma$. It is clear that for each prime divisor p of n (where $n = pq$), it is true that:

$$-1 \equiv \begin{cases} -q \pmod{p} & \text{if } (p-1)|(n-1) \\ 0 \pmod{p} & \text{otherwise} \end{cases}. \tag{19}$$

Since it is not possible that $-1 \equiv 0 \pmod{p}$, it must be the case that $(p-1) \mid (n-1)$. However, since $n-1 = pq-1 = q(p-1)+(q-1)$, it must also be true that $(p-1) \mid (q-1)$ but $q-1 = (n/p-1)$. It also follows from Equation (19) that $-1 \equiv -q \pmod{p}$, which implies that $p \mid (q-1)$.

($\Leftarrow$) Now, suppose it is the case that $(p-1) \mid ((n/p)-1)$ and $p \mid ((n/p)-1)$. Notice that n must not contain any squared terms as if it did, there would be a prime p where $p|n/p$, which contradicts $p|((n/p)-1)$.

It is clear from Equation (18) that $\sum_{k=1}^{n-1} k^{n-1} \equiv -q \pmod{p}$ using the first divisibility condition. The second divisibility condition, however, implies that $n/p = q \equiv 1 \pmod{p}$ which means that $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{p}$ for each prime divisor p of n. But, since $p \mid \left(\sum_{k=1}^{n-1} k^{n-1} + 1\right)$ for each prime divisor p of n and each of these divisors is distinct (i.e., no squared terms), it must be the case that

$$n \mid \sum_{k=1}^{n-1} k^{n-1} + 1 \Leftrightarrow \sum_{k=1}^{n-1} k^{n-1} + 1 \equiv 0 \pmod{n} \Leftrightarrow \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n},$$

or alternatively that $n \in \Sigma$, as required. ∎

Corollary 3.1 *$n \in \Sigma \Rightarrow n$ is square-free [8].*

Proof: Suppose not. Then it must be the case that for some p, $p^2|n$, and $p|((n/p)-1)$. However, since $p^2|n$, and $p|(n/p)$, then $p \nmid ((n/p)-1)$, which contradicts Theorem 3.1. ∎

Corollary 3.2 *$n \in \Sigma$ if and only if $p^2(p-1) \mid (n-p)$ for any prime divisor p of n [2].*

Proof: Theorem 3.1 states $n \in \Sigma$ if and only if $p|((n/p)-1)$, and $(p-1)|(n-1)$. Therefore, it stands to show that $p|((n/p)-1)$, and $(p-1)|(n-1)$ if and only if $p^2(p-1) \mid (n-p)$.

Since $p|((n/p)-1)$, $kp = (n/p)-1 \Leftrightarrow kp^2 = n-p$, which shows that $p^2|(n-p)$. However, note that $(p, p-1) = 1$, and $(p-1)|(n-1) = (n-p)+(p-1)$. Therefore, $p^2(p-1)|(n-p)$. ∎

Corollary 3.3 *If $n \in \Sigma$, then $(\phi(n), n) = 1$ [2].*

Proof: The assertion is obviously true if n is prime. Hence, take $n \in \Sigma$ with n composite (and square free by Corollary 3.1). Let p and q be distinct primes that divide n. Assume that $p \equiv 1 \pmod{q}$ for some $p, q|n$ (that is, a prime factor q of n divides part of $\phi(n)$). Then, since $n \in \Sigma$,

$$0 \equiv (n-1)+(1-n/q) = n - n/q = (n-q)+(q-n/q) \equiv -n/q \pmod{q},$$

which is absurd since n is square-free (Corollary 3.1). ∎

It is important to notice the link between Giuga's conjecture and other aspects of number theory. Of particular importance is the condition that if $n \in \Sigma$, then

n is a square free integer such that for any prime p that divides n, it is true that $(p-1) \mid (n/p-1)$. This condition is referred to as the Carmichael condition [8].

Definition 3.1 *A positive square-free composite integer n is said to satisfy the Carmichael condition if $(p-1) \mid ((n/p)-1)$ for every prime p where $p \mid n$. Equivalently, n satisfies the Carmichael condition if $(p-1)|(n-1)$ for all prime divisors p of n.*

Definition 3.2 *A positive square-free composite integer n is said to be Carmichael if it satisfies Fermat's Little Theorem:*

$$a^{n-1} \equiv 1 \pmod{n}, \tag{20}$$

whenever $(a,n) = 1$ and $a \leq n$. We refer to the set of Carmichael numbers greater than 2 as Γ.

In 1910, Carmichael conjectured that there are infinitely many composite integers which satisfy Equation (20) [5]. In 1994, Alford et al. [5] proved what was known as Carmichael's conjecture: there are infinitely many Carmichael numbers. Their technique involved showing that for sufficiently large n, the number of Carmichael numbers less than n is greater than $n^{2/7}$ [5]. Hence, as $n \to \infty$, so too does the number of Carmichael numbers. Pinch [28] showed that for a given n, the number of Carmichael numbers less than n is bounded above by $n \exp\left\{-\frac{\ln(n)\ln(\ln(\ln(n)))}{\ln(\ln(n))}\right\}$.

Among the most common Carmichael numbers are those of the form $(6k+1)(12k+1)(18k+1)$ where $k \in \mathbb{Z}^+$ and each of $(6k+1)$, $(12k+1)$ and $(18k+1)$ are prime. This representation gives rise to one of the largest Carmichael number ever found, having $k = 1805$ [18].

With reference to the second condition in Theorem 3.1, the following definition is used.

Definition 3.3 *A composite integer n with the property that $p \mid ((n/p) - 1)$ for all prime divisors p of n is said to be a Giuga number. The set of all Giuga numbers is denoted $\mathcal{G}$.*

Theorem 3.1 can now be restated as follows [20]:

Theorem 3.2 *$n \in \Sigma$ and is composite if and only if $n \in \Gamma \cap \mathcal{G}$.*

Giuga's conjecture asserts that $\Gamma \cap \mathcal{G} = \phi$.

3.1 Giuga Numbers and Giuga Sequences

Let p be a prime divisor of n. Then, Definition 3.3 is equivalent to the statement:

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbb{N}. \tag{21}$$

This equivalence is due to Giuga [20]. For the sake of convenience, we often refer to this expression as the sum minus product (and the associated integer as the sum minus product value).

Giuga's result, that a Giuga number is the same as an integer that satisfies Equation (21), leads to the following generalization.

Definition 3.4 *A finite increasing sequence of positive integers $\{a_1, \ldots a_m\}$ is said to be Giuga if $\sum_{i=1}^{m} \frac{1}{a_i} - \prod_{i=1}^{m} \frac{1}{a_i} \in \mathbb{N}$. If a_i is prime for each i, the sequence is said to be a proper Giuga sequence. A Proper Giuga sequence gives rise to a Giuga number $n \in \Sigma$, equal to the product of the elements in the set.*

The following generalization of Giuga's result is due to Borwein et al. [8]. Giuga's original result follows as a corollary.

Theorem 3.3 *A finite increasing sequence of positive integers* $\{a_1, \ldots a_m\}$ *satisfies*

$$a_i \mid a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_m - 1$$

for every $i \leq m$ *if and only if it is a Giuga sequence.*

Proof: Let $A = \prod_{i=1}^{m} a_i$ and define $b_i = A/a_i$. Notice that the sequence $\{a_1, \ldots, a_m\}$ is Giuga if and only if $A|(b_1 + \cdots + b_m - 1)$.

The converse is an immediate consequence of this alternative representation of a Giuga sequence.

To show the converse, assume that $a_i \mid (b_i - 1)$ or equivalently, that $a_i^2 \mid (A - a_i)$ for every i. Integer multiplication yields $A^2 \mid (A - a_1) \cdots (A - a_m)$. Ignoring all multiples of A^2 reveals that $A^2 \mid (A(b_1 + \cdots + b_m) - (a_1 \cdots a_m)) = (A(b_1 + \cdots + b_m - 1))$, which implies that $\{a_1, \ldots a_m\}$ is a Giuga sequence. ∎

Corollary 3.4 *n is a Giuga number if and only if*

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbb{N}.$$

Corollary 3.5 *[2]* $n \in \Sigma$ *if when p is a prime factor of n*

$$n \sum_{p|n} \frac{1}{p} \equiv 1 \pmod{n}.$$

Proof: Clearly, n satisfies

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbb{N}.$$

It follows that

$$n \left(\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \right) \in \mathbb{N}.$$

This gives

$$n \sum_{p|n} \frac{1}{p} - 1 \in \mathbb{N}.$$

Now, the denominator of the sum term will be n (as the product of the primes is n). This will cancel out the n in front of the sum. Hence, by Theorem 3.3,

$$n \sum_{p|n} \frac{1}{p} \equiv 1 \pmod{n}.$$

■

It is conceivable that an integer n could give rise to two different non-trivial factorizations, both of which are Giuga sequences. There is no known example of this.

If it happened to be the case that no Giuga number could also be a Carmichael number, then Giuga's conjecture would be proved. Since all Carmichael numbers are odd, if every Giuga sequence contains an even factor, then it follows that Giuga's conjecture would be proved.

The search for Giuga sequences has been completed up to and including length 8 and the results are contained in the following table [8]:

Number of Factors	**Number of Sequences**
2	None
3	One
4	Two
5	Three
6	17
7	27
8	Hundreds

Table 7: Number of Giuga Sequences

Of the Giuga sequences referred to in Table 7 only 12 are proper and those are listed in Table 8.

Even if the number of Giuga sequences of a given length seems to increase dramatically with the number of factors, the next result (which was obtained through

3 factors:
30 $= 2 \cdot 3 \cdot 5$
4 factors:
858 $= 2 \cdot 3 \cdot 11 \cdot 13$ **1722** $= 2 \cdot 3 \cdot 7 \cdot 41$
5 factors:
66198 $= 2 \cdot 3 \cdot 11 \cdot 17 \cdot 59$
6 factors:
2214408306 $= 2 \cdot 3 \cdot 11 \cdot 23 \cdot 31 \cdot 47057$ **24423128562** $= 2 \cdot 3 \cdot 7 \cdot 43 \cdot 3041 \cdot 4447$
7 factors:
432749205173838 $= 2 \cdot 3 \cdot 7 \cdot 59 \cdot 163 \cdot 1381 \cdot 775807$ **14737133470010574** $= 2 \cdot 3 \cdot 7 \cdot 71 \cdot 103 \cdot 67213 \cdot 713863$ **550843391309130318** $= 2 \cdot 3 \cdot 7 \cdot 71 \cdot 103 \cdot 61559 \cdot 29133437$
8 factors:
244197000982499715087866346 $= 2 \cdot 3 \cdot 11 \cdot 23 \cdot 31 \cdot 47137 \cdot 28282147 \cdot 3892535183$ **55479914617070801288578559178** $= 2 \cdot 3 \cdot 11 \cdot 23 \cdot 31 \cdot 47059 \cdot 2259696349 \cdot 110725121051$ **19106671814205079845555759916338506** $= 2 \cdot 3 \cdot 7 \cdot 43 \cdot 1831 \cdot 138683 \cdot 2861051 \cdot 1456230512169437$

Table 8: Proper Giuga Sequences

communication with Julian Buck and Jed Brown) guarantees that there are only finitely many sequences of any length.

Proposition 3.1 *Let m be a fixed natural number. Then there exist only finitely many Giuga sequences of length m.*

Proof: Fix m and let $\{a_1, \ldots, a_m\}$ be a Giuga sequence. From Definition 3.4,

$$\sum_{i=1}^{m} \frac{1}{a_i} > 1.$$

Furthermore, there is an element a_{j_1} such that $\frac{1}{a_{j_1}} > \frac{1}{m}$ since if this were not the case then $\sum_{i=1}^{m} \frac{1}{a_i} \leq m\frac{1}{m} = 1$, a contradiction. This implies that $a_{j_1} < m$. Therefore, there are at most m choices for a_{j_1}

Since

$$\sum_{i=1}^{m} \frac{1}{a_i} - \frac{1}{a_{j_1}} > 1 - \frac{1}{a_{j_1}} = \frac{a_{j_1} - 1}{a_{j_1}},$$

it must be the case that there is an a_{j_2} such that

$$\frac{1}{a_{j_2}} > \frac{a_{j_1} - 1}{(m-1)a_{j_1}},$$

since otherwise we would have

$$\sum_{i=1}^{m} \frac{1}{a_i} - \frac{1}{a_{j_1}} \leq (m-1)\left(\frac{a_{j_1} - 1}{(m-1)a_{j_1}}\right) = \frac{a_{j_1} - 1}{a_{j_1}},$$

another contradictory statement. So, we have $\frac{(m-1)a_{j_1}}{a_{j_1}-1} > a_{j_2}$ and because m is fixed and there are only finitely many choices for a_{j_1}, it follows that there are only finitely many choices for a_{j_2}.

All other cases follow in an analogous manner. For example, it is not difficult to show that

$$\frac{1}{a_{j_3}} > \frac{a_{j_1}a_{j_2} - a_{j_1} - a_{j_2}}{(m-2)a_{j_1}a_{j_2}},$$

and so

$$\frac{(m-2)a_{j_1}a_{j_2}}{a_{j_1}a_{j_2} - a_{j_1} - a_{j_2}} > a_{j_3},$$

implying, again that there are only finitely many cases for a_{j_3}.

In general, it must be the case that

$$a_{j_{r+1}} < \frac{(m-r)\prod_{i=1}^{r} a_{j_i}}{\prod_{i=1}^{r} a_{j_i} - \left(\sum_{i=1}^{r} \frac{\prod_{t=1}^{r} a_{j_t}}{a_{j_i}}\right)}. \tag{22}$$

Equation 22 can be shown in the following way. Suppose for $1 \leq r \leq m-1$, and $a_{j_1}, a_{j_2}, \ldots, a_{j_r}$ have all been removed from the sum. Then it is necessarily the case

that

$$\sum_{i=1}^{m} \frac{1}{a_i} - \sum_{i=1}^{r} \frac{1}{a_{j_i}} > \frac{\prod_{i=1}^{r} a_{j_i} - \left(\sum_{i=1}^{r} \frac{\prod_{t=1}^{r} a_{j_t}}{a_{j_i}}\right)}{\prod_{i=1}^{r} a_{j_i}}.$$

Again, this implies that there is an $a_{j_{r+1}}$ such that

$$\frac{1}{a_{j_{r+1}}} > \frac{\prod_{i=1}^{r} a_{j_i} - \left(\sum_{i=1}^{r} \frac{\prod_{t=1}^{r} a_{j_t}}{a_{j_i}}\right)}{(m-r)\prod_{i=1}^{r} a_{j_i}},$$

which implies the desired result that

$$\frac{(m-r)\prod_{i=1}^{r} a_{j_i}}{\prod_{i=1}^{r} a_{j_i} - \left(\sum_{i=1}^{r} \frac{\prod_{t=1}^{r} a_{j_t}}{a_{j_i}}\right)} > a_{j_{r+1}}.$$

Using the same argument as before, because of a fixed m, there are only finitely many choices for each of $a_{j_1}, \ldots, a_{j_r}$. Hence, there are only finitely many integer values for $a_{j_{r+1}}$. It follows that each $a_i \in \{a_1, \ldots, a_m\}$ may take on only a finite number of integer values. Therefore, the number of Giuga sequences of length m is finite.

■

Although the proof is rather long winded, it leads to an algorithm for finding all Giuga sequences of a given length. This algorithm can be found in Appendix 4.

Corollary 3.6 *Define*

$$\mathcal{G}_m = \{a \in \mathbb{N} | a \text{ is an element of a Giuga sequence of length } m\}.$$

For any fixed $m \in \mathbb{N}$, $\mathcal{G}_m$ has a maximal element.

It is not known if all $n \in \mathbb{N}$ could be an element of $\mathcal{G}_m$ for some m. Further, although the number of Giuga sequences of a fixed length is limited to a finite number and there is a maximal size of element for any given sequence length, we can say more. If $\{a_1, \ldots, a_m\}$ is an increasing Giuga sequence of length m then there are bounds on each term of the sequence (another result due to Hobart and Buck).

Proposition 3.2 *If $\{a_1, a_2, \ldots, a_m\}$ is a Giuga sequence with sum minus product x, then $m > a_1 x$.*

Proof: Fix a_1 and notice that for $i = 1, \ldots, m$, $\frac{1}{a_i+1} \geq \frac{1}{a_{i+1}}$ as $a_i + 1 \leq a_{i+1}$. Therefore, a sufficient condition for $\sum_{i=0}^{m-1} \frac{1}{a+i} > x$ is $\sum_{i=1}^{m} \frac{1}{a_i} > x$. This shows

$$\frac{m}{a_1} = \sum_{i=1}^{m} \frac{1}{a_1} > \sum_{i=1}^{m} \frac{1}{a_i} > x.$$

Multiply both sides by a_1 to obtain the desired result.

■

The final theorem in this section shows a bound on a_j for many different j, based solely on the choice of a_1.

Theorem 3.4 *Let m be a fixed natural number and suppose that $\{a_1, \ldots a_m\}$ is a Giuga sequence. Then for any j such that $a_1 + 1 - j > 0$, $a_j < \frac{a_1(m-j+1)}{a_1-j+1}$.*

Proof:

$$\frac{a_2 \cdots a_m + a_1 a_3 \cdots a_m + \ldots + a_1 \cdots a_{m-1}}{\prod_{i=1}^{m} a_i} > 1$$

$$\Rightarrow \frac{(j-1)a_2 \cdots a_m + (m-j+1)a_1 \cdots a_{j-1} \cdot a_{j+1} \cdots a_m}{\prod_{i=1}^{m} a_i} > 1$$

$$\Rightarrow \frac{j-1}{a_1} + \frac{m-j+1}{a_j} > 1$$

$$\Rightarrow \frac{(j-1)a_j + (m-j+1)a_1}{a_1 a_j} > 1$$

$$\Rightarrow (j-1)a_j + (m-j+1)a_1 > a_1 a_j$$

$$\Rightarrow (m-j+1)a_1 > a_1 a_j - (j-1)a_j$$

$$\Rightarrow (m-j+1)a_1 > a_j(a_1 - (j-1))$$

$$\Rightarrow \frac{(m-j+1)a_1}{a_1 - j + 1} > a_j \quad \text{whenever } a_1 + 1 - j > 0.$$

■

From a theoretical standpoint, all of these results are fairly interesting, however, from a computational point of view, they are perhaps less spectacular than one would hope. Among other problems, the results so far, by their very construction, make no attempt to discourage an exponential time increase when increasing the length of a Giuga sequence.

3.2 "The Eightfold Way"

Recall that Giuga's conjecture states that n is prime iff:

$$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}.$$

"The Eightfold Way" is a set of variants of this equation, due to Wong [57], involving Euler's phi function. These 8 similar versions of Giuga's conjecture, give insight into the requirements for counterexamples to the conjecture. Before showing the eight variations, we need to establish two important results. Theorems and proofs from this section are established in [57].

Theorem 3.5 *Let $q = p^r$ be a prime power. Then*

$$\sum_{k \in \mathbb{Z}_q^*} k^m \equiv \begin{cases} 0 \pmod{q} & \text{if } (p-1) \nmid m \\ \phi(q) \pmod{q} & \text{otherwise} \end{cases}.$$

Proof: If $q = 2$, then, $\sum_{k \in \mathbb{Z}_q^*} k^m \equiv 1 \equiv \phi(2) \pmod{2}$.

Now, suppose that $p \geq 3$. We claim that

$$\sum_{k \in \mathbb{Z}_q^*} k^m \equiv \phi(q) \pmod{q} \iff (p-1) | m.$$

Let

$$S = \sum_{k \in \mathbb{Z}_q^*} k^m = \sum_{k=0}^{\phi(q)-1} (\alpha_q^k)^m = \sum_{k=0}^{\phi(q)-1} \beta^k,$$

where α_q is a primitive root modulo q, and $\beta = \alpha_q^m$. Saying $(p-1) \nmid m$ is equivalent to $\beta - 1$ being non-zero modulo p and hence invertible modulo q. So, if $(p-1) \nmid m$, then S is a geometric series and $S = \frac{\beta^{\phi(q)}-1}{\beta-1} \equiv 0 \pmod{p}$.

Now, suppose that $(p-1)|m$. Then without loss of generality, $m = (p-1)p^{s-1}$, where $1 \leq s \leq r$, and therefore, $\beta \equiv 1 \pmod{p^s}$ by lemma 2.2. Since the order of β is $\phi(q)/m = p^{r-s}$, S consists of m repetitions of

$$T = \sum_{k=0}^{p^{r-s}-1} \beta^k.$$

Since α_p is primitive, the summands of T are distinct modulo q and are all congruent to 1 modulo p^s. Thus, they must form a permutation of the arithmetic progression $1 + mp^s$, $0 \leq m < pr - s$. The sum of the terms in this progression is

$$p^{r-s} + p^s p^{r-s}(p^{r-s} - 1)/2 = q - s + O(q),$$

which gives $T = p^{r-s}$, hence $S = mT = (p-1)p^{r-1} = \phi(q)$.

Now, when $p = 2$ and hence $q = 2^r$, then

$$\sum_{k \in \mathbb{Z}_q^*} k^m \equiv \phi(2^r) \pmod{2^r} \iff m \text{ is even.}$$

For m odd, the terms of the sum $\sum_{k \in \mathbb{Z}_q^*} k^m$ cancel out in pairs, thus

$$\sum_{k \in \mathbb{Z}_q^*} k^m \equiv 0 \pmod{2^r}.$$

Suppose m even. Without loss of generality, we can take $1 \leq s \leq r-2$. Then

$$S = (1 + (-1)^m) \sum_{k=1}^{(2^r/4)-1} \beta^k,$$

where $\beta = 5^m$. Since m is even, the first factor is 2. The second factor consists of m repetitions of

$$T = \sum_{k=0}^{(2^r/4m)-1} \beta^k.$$

The summands of T are distinct modulo 2^r and congruent to 1 modulo $4m$. Therefore, they form a permutation of the arithmetic progression $1 + 4mn$, $0 \leq n < 2^r/4m$, which sums to

$$2^r/4m + 4m(2^r/4m)(2^r/4m - 1)/2 = 2^r/4m + O(2^r/2).$$

Multiplication by $2m$ yields $S = 2mT = 2^r/2 = \phi(2^r)$. ∎

Theorem 3.6 *If $m > 1$, then*

$$\sum_{k \in \mathbb{Z}_q^*} k^m \equiv \sum_{k \in \mathbb{Z}_q} k^m \pmod{q}.$$

When p is odd, the congruence holds for $m \geq 1$.

Proof: When $m > r$ this is a trivial result obtained by applying Fermat's Little Theorem and noticing that the orders of the groups are the same modulo q. Thus,

use $r = 1$ as the base case and proceed by induction. For $r > 1$,

$$\sum_{k \in \mathbb{Z}_q} k^m = \sum_{k \in \mathbb{Z}_q^*} k^m + p^m \sum_{k \in \mathbb{Z}_{p^{r-1}}} k^m.$$

Since the last term is divisible by $p^m p^{r-2}$,

$$\sum_{k \in \mathbb{Z}_q} k^m \equiv \sum_{k \in \mathbb{Z}_q^*} k^m \pmod{q}.$$

When $m = 1$,

$$\sum_{k \in \mathbb{Z}_q} k - \sum_{k \in \mathbb{Z}_q^*} k = \sum_{k=1}^{p^{r-1}} pk = \frac{1}{2} q p^{r-1} + 1,$$

which is divisible by q if p is odd. ∎

We are now in a position to develop the eight general equations related to Giuga's conjecture. The first result is a generalization of Theorem 3.1. The next two results follow trivially.

Theorem 3.7 $\sum_{k \in \mathbb{Z}_n} k^m \equiv -1 \pmod{n}$ *if and only if* n *is square free and for each prime divisor of* n, *we have* $(p-1)|m$ *and* $p|((n/p)-1)$

Proof: We begin by showing that n is square free. Suppose that $q|n$ where $p|n$ and q is a prime power of p. In particular, this means that $p^2|n$. Then $p|\phi(q)$, and hence,

$$\sum_{k \in \mathbb{Z}_n} k^m \equiv 0 \neq -1 \pmod{q}.$$

In a similar way, we require $\sum_{k \in \mathbb{Z}_p} k^m$ to be non-zero modulo p. Hence, the condition that $(p-1)|m$ for odd p follows from Theorem 3.5. If $p = 2$, the congruence is trivial.

The third condition is met when we consider

$$\sum_{k \in \mathbb{Z}_n} k^m \equiv (n/p)\phi(p) \equiv -1 \pmod{p}.$$

Dividing the equation by $\phi(p) = p - 1 \equiv -1 \pmod{p}$, we get $n/p \equiv 1 \pmod{p}$, or $p|((n/p) - 1)$, as required. ∎

Corollary 3.7 $\sum_{k \in \mathbb{Z}_n} k^{\phi(n)} \equiv -1 \pmod{n}$ *if and only if* n *is square free and for each prime* p *dividing* n, $p|((n/p) - 1)$.

Corollary 3.8 (Giuga) $\sum_{k \in \mathbb{Z}_n} k^{n-1} \equiv -1 \pmod{n}$ *if and only if* n *is square free and for each prime* p *dividing* n, $p|((n/p) - 1)$ *and* $(p-1)|((n/p) - 1)$.

After examining the two cases where the exponent on k is $n - 1$ and $\phi(n)$, we consider the cases arising from changing the modulus.

Theorem 3.8 $\sum_{k \in \mathbb{Z}_n} k^m \equiv \phi(n) \pmod{n}$ *if and only if for every* $1 \leq i \leq l$, *one of the following conditions holds:*

- $\sum_{k \in \mathbb{Z}_q} k^m \equiv 0 \pmod{q}$ *and* $p|q - 1$ *for* $p, q|n$; *or*
- $\sum_{k \in \mathbb{Z}_q} k^m \equiv \phi(q) \pmod{q}$ *and* $n|q \equiv \phi(n/q) \pmod{q}$.

Proof: For the first case, consider $\phi(q)\phi(n/q) \equiv 0 \pmod{q}$. This is equivalent to $p|\phi(n/q)$, which is in turn equivalent to $p|(q-1)$ for all p and $q|n$.

In the second case, we must have $(n/q)\phi(q) \equiv \phi(n) \equiv \phi(q)\phi(n/q) \pmod{q}$. Since $\phi(q)$ is divisible by p^{r-1}, we can divide through by $\phi(q)$ to get $(n/q) \equiv \phi(n/q) \pmod{p}$. ∎

Corollary 3.9 $\sum_{k \in \mathbb{Z}_n} k^{\phi(n)} \equiv \phi(n) \pmod{n}$ *if and only if for all primes* p *dividing* n, *it is the case that* $n/q \equiv \phi(n/q)$, *for all* $q||n$.

Corollary 3.10 $\sum_{k \in \mathbb{Z}_n} k^{n-1} \equiv \phi(n) \pmod{n}$ *if and only if* $n = 2$ *or* n *is odd,* $n/q \equiv \phi(n/q) \pmod{p}$ *and* $(p-1)|(n-1)$ *for all primes* $p|n$, *and* $q||n$.

Proof: Suppose that for some prime p, $p|(n-1)$, so $\sum_{k\in \mathbb{Z}_q} k^{n-1} \equiv 0 \pmod{q}$. Select q to be maximal. Then there must be a $q|n$ such that $p|(q-1)$. Clearly, $p \not|(n-1)$ so $(q-1) \not|(n-1)$. Since $q > p$, this is a contradiction. ∎

It is clear that $\mathbb{Z}_n^*$ is a group under multiplication. We need some further information about the structure of this group. Indeed, $\mathbb{Z}_n^*$ is isomorphic to the Cartesian product $\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ [57]. Define $\mathbb{Z}_n^{*i}$ to be the set of elements of $\mathbb{Z}_p^*$ which are congruent to 1 modulo n/q_i. This set has cardinality of $\phi(q_i)$, and contains a unique representative modulo q_i for each element in $\mathbb{Z}_{q_i}^*$. By applying the Chinese Remainder Theorem, we obtain the following fact [57], which we will require later:

Theorem 3.9 *Every $x \in \mathbb{Z}_n^*$ can be written uniquely as a product $x \equiv x_1 x_2 \cdots x_l \pmod{n}$ with each $x_i \in \mathbb{Z}_n^{*i}$.*

Proof: Since $\prod_{i=1}^{l} x_i \equiv x_i \pmod{q}$, x_i must be the unique element of $\mathbb{Z}_n^{*i}$ which is congruent to x modulo q. ∎

Using this representation, we can factor $S = \sum_{k\in \mathbb{Z}_n^*} k^m$ into $S_1 S_2 \cdots S_l$ where

$$S_i = \sum_{k\in \mathbb{Z}_n^{*i}} k^m.$$

Since $S_i \equiv \phi(q_j) \pmod{q_j}$ whenever $j \neq i$, we are only interested in the S_i congruent to $\sum_{k\in \mathbb{Z}_{q_j}^*} k^m$ modulo q_j. Theorem 3.5 gives

$$S_i \equiv \begin{cases} 0 \pmod{q_i} & \text{if } (p-1) \not| m \\ \phi(q_i) \pmod{q_i} & \text{otherwise} \end{cases}.$$

Therefore,

$$S = \prod_{i=1}^{l} S_i \equiv \begin{cases} 0 \pmod{q_i} & \text{if } (p-1) \not| m \\ \phi(q_i) \prod_{i\neq j} \phi(p_j^{r_j}) \equiv \phi(n) \pmod{q_i} & \text{otherwise} \end{cases}.$$

This representation gives rise to the next theorem.

Theorem 3.10 $S = \sum_{k \in \mathbb{Z}_n^*} k^m \equiv -1 \pmod{n}$ *if and only if* n *is prime and* $(n-1)|m$.

Proof: Since $(n-1, n) = 1$, it must not be the case that $S_i \equiv 0 \pmod{q_i}$, for any i. Therefore, $S_i \equiv \phi(q_i)$ for all i, so that $S = \phi(n)$. However, $\phi(n) < n - 1$ whenever n is not prime. The result then follows from Theorem 3.5. ∎

Corollary 3.11 $S = \sum_{k \in \mathbb{Z}_n^*} k^{\phi(n)} \equiv -1 \pmod{n}$ *if and only if* n *is prime.*

Corollary 3.12 $S = \sum_{k \in \mathbb{Z}_n^*} k^{n-1} \equiv -1 \pmod{n}$ *if and only if* n *is prime.*

Theorem 3.11 $S = \sum_{k \in \mathbb{Z}_n^*} k^m \equiv \phi(n) \pmod{n}$ *if and only if for each* i, *either* $\sum_{k \in \mathbb{Z}_{q_i}^*} k^m \equiv \phi(q_i) \pmod{q_i}$, *or* $p_i|(p_j - 1)$ *for some* $p_j|n$.

Proof: If $S = \sum_{k \in \mathbb{Z}_n^*} k^m \equiv 0 \pmod{q_i}$, then we need $\phi(n) \equiv 0 \pmod{q_i}$ which implies the second condition.

If $S = \sum_{k \in \mathbb{Z}_n^*} k^m \equiv \phi(q_i) \pmod{q_i}$, then we have $\sum_{k \in \mathbb{Z}_n^*} k^m \equiv \phi(q_i) \pmod{q}$ by the argument before the theorem. ∎

The final two corollaries for this section complete the set of variants of Giuga's conjecture. They follow naturally from the previous theorem.

Corollary 3.13 $S = \sum_{k \in \mathbb{Z}_n^*} k^{\phi(n)} \equiv \phi(n) \pmod{n}$ *for all* $n \in \mathbb{N}$.

Corollary 3.14 $S = \sum_{k \in \mathbb{Z}_n^*} k^{n-1} \equiv \phi(n) \pmod{n}$ *if and only if* $n = 2$ *or* n *is odd and* $(p-1)|(n-1)$ *for each prime divisor of* n.

Proof: n must satisfy $(p-1)|(n-1)$ by the same argument as Corollary 3.10. As in that same Corollary, the condition does not hold when n is a power of two, so n cannot be even. By Theorem 3.11, the condition is sufficient. ∎

Table 9 summarizes the eight different variants of

$$\sum_{k \in I} k^m \equiv r \pmod{n}. \tag{23}$$

I	r	m	Conditions on n	Corollary
$\mathbb{Z}_n$	$n-1$	$\phi(n)$	$p\|((n/p)-1)$ for all prime divisors p of n.	3.7
$\mathbb{Z}_n$	$n-1$	$n-1$	n is square-free, $p\|((n/p)-1)$ and $(p-1)\|((n/p)-1)$ for all prime divisors p of n.	3.8
$\mathbb{Z}_n$	$\phi(n)$	$\phi(n)$	$n/q \equiv \phi(n/q) \pmod{p}$ for all $p\|n$ where $q\|\|n$.	3.9
$\mathbb{Z}_n$	$\phi(n)$	$n-1$	n is odd, $n/q \equiv \phi(n/q) \pmod{p}$, $(p-1)\|(n-1)$ for all $p\|n$ where $q\|\|n$.	3.10
$\mathbb{Z}_n^*$	$n-1$	$\phi(n)$	Prime	3.11
$\mathbb{Z}_n^*$	$n-1$	$n-1$	Prime	3.12
$\mathbb{Z}_n^*$	$\phi(n)$	$\phi(n)$	Every $n \in \mathbb{N}$	3.13
$\mathbb{Z}_n^*$	$\phi(n)$	$n-1$	n is odd and $(p-1)\|(n-1)$ for all prime divisors p of n.	3.14

Table 9: The "Eightfold Way"

The next section looks at the conditions for these equivalences to hold. We will develop the theory of normal families of primes, co-Giuga numbers and pseudo-Carmichael numbers and how they relate to equation 23.

3.3 Normal Families, Co-Giuga, and Pseudo-Carmichael Numbers

Normal families of primes are important in the study of Giuga's conjecture for a number of reasons. First, any counterexample to Giuga's conjecture must be normal (because of the Carmichael condition). Second, the normal family condition on the counterexample allows significant computational work to be done on Giuga's conjecture. This section outlines some results on normal families of primes as well as the theory of co-Giuga numbers and pseudo-Carmichael numbers. This will conclude

the development of Wong's Eightfold way and provide a lead in to some important computational results. Results in this section stem primarily from the work of Wong [57].

3.3.1 Normal Families of Primes

Any counterexample, n, to Giuga's conjecture must satisfy $p_i \nmid (p_j - 1)$ for any two prime divisors of n. Indeed, if $p_i|(p_j - 1)$, then there is a k such that $kp_i + 1 = p_j$ and so

$$p_j - 1 = ((kp_i + 1) - 1)|(n - 1) \quad \text{and} \quad p_j|n.$$

This contradicts Theorem 3.1. The prime factors of such an integer give rise to a set which is called normal.

Definition 3.5 *A finite family P of distinct primes is called normal if*

$$p_i \nmid (p_j - 1),$$

for every p_i and p_j.

Example 6 *The set $\{3, 5, 17\}$ is normal while the set $\{3, 7, 13\}$ is not because $3|13-1$ and $3|7 - 1$.*

Using the power of Sylow's theorems, we have the following results about normal families. The result is due to Holt, and can be found in Wong [57].

Theorem 3.12 *Suppose $P = \{p_1, p_2, \ldots, p_m\}$ is a normal family of primes and let $n = p_1 p_2 \cdots p_m$. Then there is a unique group of order n up to isomorphism.*

Proof: Let G be a group of order n. If $P = \{p_1, p_2 \ldots p_m\}$ is a Sylow p-subgroup of G, then $|\mathrm{Aut}(P)| = p - 1$ does not divide $|G|$. Applying the Burnside Transfer

Theorem shows that G has a normal subgroup N of order n/p_i such that $G = NP$. Choosing P to be a normal Sylow p-subgroup of G, we see that $G \cong N \times P$. Induction on m completes the argument. ∎

Theorem 3.13 *If n is divisible by primes p_i, p_j for which $p_i|(p_j - 1)$, then there exists a non-cyclic group of order n.*

Proof: It is sufficient to find non-cyclic groups of orders p^2 and pq. $\mathbb{Z}_p \times \mathbb{Z}_p$ suffices for a group of order p^2. For a group of order pq, let b be a primitive $p - th$ root of unity modulo q. Then the group with presentation $\langle x, y | x^p = y^q = 1, xy = y^b x \rangle$ is non-Abelian and of order pq. ∎

As stated previously, any counterexample to Giuga's conjecture must be normal. Other well-known unsolved problems in number theory revolve around the normal condition as well (for example Lehmer's conjecture). For a more detailed reference, please see Guy's book, Unsolved Problems in Number Theory [21].

3.3.2 Pseudo-Carmichael Numbers

We noted earlier (Corollary 3.14) that an integer n satisfies

$$\sum_{k \in \mathbb{Z}_n^*} k^{n-1} \equiv \phi(n) \pmod{n}$$

if and only if $n = 2$ or n is odd and $(p-1)|(n-1)$ for each prime divisor of n. The condition that $(p-1)|(n-1)$ is known as the pseudo-Carmichael condition [57].

Definition 3.6 *An integer n is said to be pseudo-Carmichael if for every prime divisor p of n, $(p-1)|(n-1)$.*

The pseudo-Carmichael number condition is identical to the Carmichael condition; the difference between a Carmichael number and a pseudo-Carmichael number is that

n is not required to be square-free. Hence, every Carmichael number is also pseudo-Carmichael. Since there are infinitely many Carmichael numbers, it follows that there are infinitely many pseudo-Carmichael numbers.

The following theorem provides a link between normal families of primes and pseudo-Carmichael numbers.

Theorem 3.14 *Let $P = \{p_1, p_2, \ldots, p_l\}$ be a normal family of primes, and define $r_i = lcm_{i \neq j}(\phi(p_j))$. Then any number of the form $p_1^{k_1 r_1} p_2^{k_2 r_2} \cdots p_l^{k_l r_l}$ with $k_i \in \mathbb{Z}^+$ is pseudo-Carmichael. Conversely, if n is pseudo-Carmichael, then its prime factors form a normal family.*

Proof: Since $\phi(p_j) | r_i$ whenever $j \neq i$, it must be the case that $p_i^{k_i r_i} \equiv 1 \pmod{p_j - 1}$, by Euler's generalization of Fermat's Little Theorem. In the case that $i = j$,

$$p_i^{k_i r_i} \equiv 1 \pmod{p_i - 1}$$

holds trivially. Therefore, whenever

$$n = \prod_{i=1}^{l} p_i^{r_i k_i} \equiv 1 \pmod{p_j - 1},$$

$(p_j - 1) | (n - 1)$, for all j.

Conversely, suppose that n is pseudo-Carmichael but the prime divisors do not form a normal family. As n is pseudo-Carmichael, it must be the case that $(q-1) | (n-1)$, which implies that

$$(q - 1)l = n - 1, \quad l \in \mathbb{Z}.$$

Further, the condition that the factors of n are non normal implies $p | (q - 1)$ or that

$$pm = q - 1, \quad m \in \mathbb{Z}.$$

These conditions together imply $p | (n - 1)$ which is absurd as $p | n$. ∎

3.3.3 Co-Giuga Numbers

As was the case with pseudo-Carmichael numbers, we can define a class of integers whose characterization is similar to that of a Giuga number [57].

Definition 3.7 *An integer n is said to be co-Giuga if for all primes p dividing n and all $q = p^r || n$ it is the case that $n/q \equiv \phi(n/q) \pmod{p}$.*

Clearly from the definition, co-Giuga numbers need not be square-free while the same cannot be said for Giuga numbers. It is also true that the prime factors of a co-Giuga number must form a normal family. If this were not the case, then for some prime divisor p,

$$\phi(n/q) \equiv 0 \not\equiv n/q \pmod{p}.$$

Recall that a Giuga number, n, satisfies the equation

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in \mathbb{Z}.$$

A similar characterization applies to co-Giuga numbers. Since the co-Giuga condition is independent of the exponent on p, we can consider only square-free numbers without any loss of generality.

Theorem 3.15 *n is co-Giuga if and only if*

$$\prod_{p|n} \left(\frac{1}{p} - 1\right) - \sum_{p|n} \left(1 - \frac{1}{p}\right) \in \mathbb{Z}.$$

Proof: Suppose that $n = p_1 p_2 p_3$ (a similar argument works for more prime divisors). Then,

$$(p_2 - 1)(p_3 - 1) \equiv p_2 p_3 \pmod{p_1}$$

$$(p_1 - 1)(p_3 - 1) \equiv p_1 p_3 \pmod{p_2}$$

$$(p_2 - 1)(p_1 - 1) \equiv p_2 p_1 \pmod{p_3}.$$

Which means that:

$$(p_1-1)(p_2-1)(p_3-1) \equiv p_2p_3(p_1-1) \pmod{p_1}$$

$$(p_1-1)(p_2-1)(p_3-1) \equiv p_1p_3(p_2-1) \pmod{p_2}$$

$$(p_1-1)(p_2-1)(p_3-1) \equiv p_1p_2(p_3-1) \pmod{p_3}.$$

Using the Chinese Remainder Theorem (Theorem 2.4), it is clear that there is a unique solution to this system given by

$$(p_1-1)(p_2-1)(p_3-1) \equiv -p_2p_3 - p_1p_3 - p_1p_2 \pmod{n}.$$

This formulation, however, is equivalent to

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)+\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3} \in \mathbb{Z},$$

or alternatively,

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)-\left(1-\frac{1}{p_1}\right)-\left(1-\frac{1}{p_2}\right)-\left(1-\frac{1}{p_3}\right) \in \mathbb{Z}.$$

A similar argument can be used to prove the theorem on an arbitrary number of divisors. ∎

In his paper, Wong [57] showed that there is no non-trivial co-Giuga number with fewer than 7695 prime factors. We conclude this section with Wong's original proof as well as Wong's original representation of the "Eightfold way", illustrated in Table 10.

Definition 3.8 *Given two families of primes* $A = \{p_1, p_2, p_3, \cdots, p_k\}$ *and* $B = \{q_1, q_2, q_3, \cdots, q_l\}$, *with* $p_i < p_j$ *and* $q_i < q_j$ *whenever* $i < j$, *we say that* A *dominates* B *if* $k \geq l$ *and* $p_i \leq q_i$ *for every* $1 \leq i \leq l$.

Theorem 3.16 *There are no non-trivial co-Giuga numbers with fewer than 7695 prime factors.*

Proof: Let $P = \{p_1 < p_2 < p_3 < \ldots\}$ be a normal sequence of primes. Consider the expression

$$d(P,l) = \prod_{i=1}^{l}\left(1 - \frac{1}{p_i}\right) + \sum_{i=1}^{l}\frac{1}{p_i} - 2, \quad l \in \mathbb{Z}^+.$$

It is clear from Theorem 3.15 that $n = \prod_{i=1}^{l} p_i$ is a co-Giuga number if $d(P,l) \in \mathbb{Z}$. If $l = 1$, then $d(P,l) = -1$. Notice also that d is monotonically increasing (in the strict sense). The function is also monotonically increasing in p_i. This implies that if Q is a normal family that dominates P, and $m \leq l$, then $d(Q,l) \geq d(P,m)$.

Now, P is dominated by one of the following two sequences [57]:

$$A = \{5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}, \quad \text{or}$$

$$B = \{3, 5, 11, 17, 23, 29, 41, \ldots\}.$$

However, $d(A, 7694) = -0.000094$ while $d(B, 7694) = -0.4071613\ldots$, implying that $-1 < d(P,m) < 0$ for $m < 7695$. Thus, d cannot be an integer.

■

3.4 Computational Results

3.4.1 Counterexamples

Using the property that any counterexample to Giuga's conjecture must be a Carmichael number, it is clear that the smallest counterexample is greater than 560 as

$$561 = 3 \cdot 11 \cdot 17$$

is the smallest $n \in \Gamma$. When he wrote his original paper [20], however, Giuga used the the Carmichael condition along with the Giuga condition to show that the smallest counterexample would require at least 1,000 digits. As computational power

I	r	m	Conditions on n	Trivial cases	Non-Trivial examples	Corollary
$\mathbb{Z}_n$	$n-1$	$\phi(n)$	Giuga	Primes	30, 858, 1722, etc.	3.7
$\mathbb{Z}_n$	$n-1$	$n-1$	Giuga and Carmichael	None	$> 13,800$ digits	3.8
$\mathbb{Z}_n$	$\phi(n)$	$\phi(n)$	Co-Giuga	Prime powers	> 7694 Prime Factors	3.9
$\mathbb{Z}_n$	$\phi(n)$	$n-1$	Odd, Co-Giuga and Pseudo-Carmichael	Odd Prime Powers	> 7694 Prime Factors	3.10
$\mathbb{Z}_n^*$	$n-1$	$\phi(n)$	Prime	Primes	None	3.11
$\mathbb{Z}_n^*$	$n-1$	$n-1$	Prime	Primes	None	3.12
$\mathbb{Z}_n^*$	$\phi(n)$	$\phi(n)$	All $n \in \mathbb{N}$	All $n \in \mathbb{N}$	None	3.13
$\mathbb{Z}_n^*$	$\phi(n)$	$n-1$	Odd and Pseudo-Carmichael	Odd Prime Powers	Carmichael Numbers, 45, 225, 325, ...	3.14

Table 10: Conditions for $\sum_{k\in I} k^m \equiv r \pmod{n}$ [57].

increased, the estimated lower bound increased to 1,700 digits (Bedocchi [6]) and most recently to 13,800 digits [8]. This section will outline the computational work that has been done on Giuga's conjecture as well as some ideas for future research in the area.

Two conditions are obvious for a sequence of primes $P = \{p_1, p_2 \ldots, p_k\}$ to form a counterexample to Giuga's conjecture.

- P is a normal family.
- $\sum_{i=1}^{k} \frac{1}{p_i} > 1$.

Define S_m to be the set of all normal sets with maximum element smaller than the m^{th} prime, p_m. For any $S \in S_m$, with $S = \{p_1, p_2 \ldots, p_k\}$, define $T_m(S) = \{p_1, p_2 \ldots, p_k, p_{k+1}, \ldots, p_r\}$ to be the smallest set of odd primes which contains S, and for every $p_j \geq p_m$ (the m^{th} prime) and $S \cup \{p_j\}$ is normal for $j > k$, and for

which $\sum_{j=1}^{r} \frac{1}{p_j} > 1$. Define $r_m(S)$ as the number of elements of $T_m(S)$.

Finally, define a sequence $\{i_m | m \in \mathbb{N}, \imath_m = \min\{r_m(S) | S \in S_m\}\}$. Giuga used the fact that this sequence is non-decreasing to calculate that a counterexample to his conjecture would have to have more than 1000 digits.

Now, the number of prime factors in a counterexample must exceed $i_m \; \forall \; m \in \mathbb{N}$. It is clear that the prime factors form a normal family. Further, each subset S of factors less than p_m is a member of S_m. Since any normal set of primes which contains S and satisfies the second condition above must have at least $r_m(S)$ elements, we have that n has at least $r_m(S) \geq i_m$ prime factors (for any $m \in \mathbb{N}$). So, any counterexample is larger than $\prod_{j=1}^{i_m} p_j$ and therefore has at least the same number of digits as this product.

After Giuga showed that a counterexample had over 1000 digits [20], Bedocchi [6] computed $i_9 = 544$ which implies that a counterexample must have over 1700 digits. Borwein et al. computed $i_{19} = 835$ with a similar algorithm, before looking for something better due to the significant slowdown resulting from exponential growth [8].

With the following observation, Borwein et al were able to compute $i_{135} = 3459$ which implies that a counterexample must have at least 13,887 digits [8].

Proposition 3.3 *Consider $S \in S_m$ and the value of $r_m(S)$. S has at most two "successors" S and S^* in the set S_{m+1}. They are S and $S^* = S \cup \{p_m\}$. It is then true that $r_{m+1}(S) \geq r_m(S)$ and $r_{m+1}(S^*) \geq r_m(S)$.*

Proof: There are two cases to consider: $S \cup \{p_m\}$ is normal, and $S \cup \{p_m\}$ is not normal.

CASE 1: $S \cup \{p_m\}$ is normal. Then S has the two successors S and S^* in S_{m+1}. Further, we have $p_m \in T_m(S)$. However, $p_m \notin T_{m+1}(S)$, but every other element is

contained in $T_{m+1}(S)$. So, $T_{m+1}(S)$ must contain at least one higher prime for the sum $\sum_{p \in T_{m+1}(S)} \frac{1}{p}$ to exceed 1. Therefore, $r_{m+1}(S) \geq r_m(S)$. S^*, the set $T_m(S)$ may contain primes which are congruent to 1 (mod p_m). These are missing in $T_{m+1}(S^*)$, since $p_m \in S^*$. For each of these, we need at least one higher prime for the sum $\sum_{p \in T_{m+1}(S^*)} \frac{1}{p}$ to exceed 1. Again, $r_{m+1}(S^*) \geq r_m(S)$.

CASE 2: $S \cup \{p_m\}$ is not normal. Then the only successor of S in S_{m+1} is S itself. Also, $T_m(S) = T_{m+1}(S)$ as the prime P_m is not contained in either set. Therefore, $r_m(S) = r_{m+1}(S)$. ∎

This shows, among other things, that the sequence i_m is non-decreasing. It also shows that the values $r_{k+1}, r_{k+2}, \ldots$ for all of the successors in $S_{k+1}, S_{k+2}, \ldots$ of a given set $S \in S_k$ do not fall below $r_k(S)$. If we want to compute i_m and already know a bound $I \geq i_m$, then we do not have to look at any successor in the sets $S_{k+1}, \ldots S_m$ of a set $S \in S_k$ with $r_k(S) > I$. The natural way to do this is iteratively.

Algorithm 3.1 *Take $A_1 = S_1$ and let A_{k+1} consist of all successors in S_{k+1} of all $S \in A_k$ with $r_k(S) \leq I$. Then $i_m = \min\{r_m(S) | S \in A_m\}$.*

If I is close to i_m, then this significantly reduces the number of sets to consider.

The bound I can be chosen as the value of $r_m(S)$ for some $S \in S_m$. The iterative method saves the most time if one correctly guesses which sets have low values. By looking at preliminary computational results, the following seems to hold [8].

Conjecture 3.1 *Let $L_5 = \{5, 7\}$, and define*

$$L_{k+1} = \begin{cases} L_k \cup \{p_k\} & \text{if } L_k \cup \{p_k\} \text{ is normal} \\ L_k & \text{otherwise} \end{cases}.$$

Then, for $m \geq 5$, $r_m(L_m) = i_m$.

This conjecture holds true for $m \leq 135$.

3.4.2 Giuga Sequences

Finding all sequences of a given length is not difficult, in theory, as all one is required to do is compute the sets of all a_i that satisfy the inequality $\sum_{i=1}^{k} \frac{1}{a_i} > 1$. To reach a Giuga number whose sum minus product value is two requires a great deal more effort than a number with sum minus product value of one. In fact, a proper Giuga sequence with sum minus product value of two requires at least 59 prime factors. Therefore, since no such Giuga number has been found (and it is not clear if one exists at this point), we will limit our discussion to sequences with sum minus product value of one.

Computing all sequences of a given length is difficult in practice. There are hundreds of sequences of length 7, and because of the exponential growth of the size of the sets, further computations are impractical. Given an initial sequence of length $m-2$ however, it is possible to find a Giuga sequence of length m.

Theorem 3.17 *[8] Let $A = \{a_1, a_2, \ldots, a_{m-2}\}$ be any sequence of length $m-2$. Let*

$$P = a_1 a_2 \cdots a_{m-2}, \quad S = \frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_{m-2}}.$$

Fix an integer $v > S$. Take any integers x, y with $x \cdot y = P(P + S - v)$ and $y > x$. Let

$$a_{m-1} = \frac{P + x}{P(v - S)}, \quad a_m = \frac{P + y}{P(v - S)}.$$

Then,

$$S + \frac{1}{a_{m-1}} + \frac{1}{a_m} - \frac{1}{P a_{m-1} a_m} = v.$$

Hence, $A \cup \{a_{m-1}, a_m\} = \{a_1, a_2, \ldots, a_{m-2}, a_{m-1}, a_m\}$ is a Giuga sequence if and only if $a_{m-1} \in \mathbb{N}$.

Proof: We begin by showing that

$$S + \frac{1}{a_{m-1}} + \frac{1}{a_m} - \frac{1}{Pa_{m-1}a_m} = v.$$

Clearly,

$$S + \frac{P(v-S)}{(P+x)} + \frac{1}{a_m} - \frac{1}{Pa_{m-1}a_m} = v.$$

as

$$S + \frac{P(v-S)}{P+x} + \frac{P(v-S)}{P+y} - \frac{P^2(v-S)^2}{P(P+x)(P+y)} = v$$

if and only if

$$\frac{P}{P+x} + \frac{P}{P+y} - \frac{P(v-S)}{(P+x)(P+y)} = 1$$

if and only if

$$\frac{P}{P+x} + \frac{P}{P+y} - \frac{P^2-xy}{(P+x)(P+y)} = 1$$

which is of course true.

This means that the extended sequence is Giuga if and only if both a_{m-1} and a_m are integers. Now, a_{m-1} is an integer if and only if a_m is an integer. Because of symmetry, it is enough to show the implication in one direction. If

$$P(v-S)|(P+x),$$

then

$$P(v-S)|(P+x)(P+y) = 2P^2 + (x+y)P - (v-S)P,$$

so

$$P(v-S)|(2P^2 + (x+y)P) = P(P+x+P+y),$$

so

$$P(v-S)|P(P+y)$$

since $P(v-S)|P+x$.

To show that $(P(v-S),P)=1$ (which would prove the assertion), assume that this is not the case. That is, there exists a prime p such that $p|P(v-S)$ and $p|P$. So, $p|a_i$ for some i only because $(a_i,a_j)=1$ when $i\neq j$. Since p divides

$$P(v-S)=vP-(a_2\cdots a_{m-2}+\ldots+a_1\cdots a_{m-3}),$$

we can drop all terms on the right hand side with a factor of a_i to get

$$p|(a_1\cdots a_{i-1}\cdot a_{i+1}\cdots a_{m-2})$$

which is a contradiction. ∎

Theorem 3.18 *[8] If $\{a_1,a_2,\ldots,a_{m-1},a_m\}$ is a Giuga sequence with sum minus product v, and if we define*

$$x=a_{m-1}P(v-S)-P,\quad y=a_mP(v-S)-P,$$

(with P and S as in the previous theorem), then x and y are integers and

$$x\cdot y=P(P+S-v).$$

Proof: Clearly, x and y are integers. It remains to show that $x\cdot y=P(P+S-v)$. We have

$$\begin{aligned}x\cdot y&=-P^2(v-S)(a_{m-1}+a_m)+P^2(a_{m-1}a_m)(v-S)^2+P^2\\&=P^2(S-v)a_{m-1}a_m(\frac{1}{a_{m-1}}+\frac{1}{a_m}+S-v)+P^2\\&=P^2(S-v)a_{m-1}a_m\frac{1}{a_{m-1}a_mP}+P^2\\&=P(P+S-v).\end{aligned}$$

∎

A counterexample to Giuga's conjecture would have to be an odd number. Hence, no member of a Giuga sequence (which is a counterexample) would be even. No such sequence has been found (counterexample or otherwise). We have the following result, however, on the relationship between n and v [8].

Proposition 3.4 *Let $n = p_1 p_2 \cdots p_m$ be an odd Giuga number. Then,*

$$m - v \equiv 1 \pmod 4.$$

Proof: Consider the Giuga sequence equation:

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_m} - \frac{1}{n} = v$$
$$\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_m} - 1 = nv$$

The result follows from considering the equation modulo 4. Indeed, assume that the first k factors are congruent to -1 modulo 4 and the other $m-k$ factors are congruent to 1 modulo 4. Then, we have

$$-1 \equiv v(-1)^k - k(-1)^{k-1} - (m-k)(-1)^k = (-1)^k(v - m + 2k) \pmod 4.$$

It easily follows that $m - v \equiv -1 \pmod 4$. ∎

In addition to being able to create Giuga sequences of length m from any sequence of length $m-2$, we also have an explicit method of creating Giuga sequences of length $m+1$ from a Giuga sequence of length m with a certain property [8].

Theorem 3.19 *Suppose a Giuga sequence $\{a_1, \ldots, a_m\}$ satisfies*

$$a_m = a_1 \cdots a_{m-1} - 1$$

and let

$$\widetilde{a}_m = a_1 \cdots a_{m-1} + 1, \quad \widetilde{a}_{m+1} = a_1 \cdots a_{m-1}\widetilde{a}_m - 1.$$

Then, $\{a_1, \ldots, a_{m-1}, \widetilde{a}_m, \widetilde{a}_{m+1}\}$ *is a Giuga sequence with the same sum minus product value.*

Proof: Let $P = a_1 \cdots a_{m-1}$ and let $S = 1/a_1 + \ldots 1/a_{m-1}$. Then, $a_m = P - 1$, $\widetilde{a}_m = P + 1$ and $\widetilde{a}_{m+1} = P^2 + P - 1$. Both sequences have the same sum minus product value if and only if

$$S + \frac{1}{P-1} - \frac{1}{P(P-1)} = S + \frac{1}{P+1} + \frac{1}{P^2+P-1} - \frac{1}{P(P+1)(P^2+P-1)},$$

which is true for all S and P. ∎

Notice that the sequences derived from this theorem are not the only ones that exist. To find all of the sequences of a given length, we can use Theorem 3.17 or Theorem 3.1. For an explicit algorithm (due to Brown, Buck and Hobart), see Appendix 5.

3.5 Agoh's Conjecture and Related Results

This section will build on the results obtained in the study of the Eightfold way. The variations discussed here are due largely to Agoh. In fact, Theorem 3.20, of this section was originally found by Agoh in his paper "On Giuga's Conjecture" [2].

Recall the two types of sums discussed in Section 3.2

$$\sum_{k \in \mathbb{Z}_n} k^m \text{ and } \sum_{k \in \mathbb{Z}_n^*} k^m.$$

These two sums along with some Bernoulli number properties play a large role in what is to follow. Specifically, note:

(I) $\sum_{k \in \mathbb{Z}_n} k^m = \sum_{k \in \mathbb{Z}_{m+1}} \frac{1}{k}\binom{m}{k-1}(n+1)^k B_{m+1-k}$,

(II) $\sum_{k \in \mathbb{Z}_n^*} k^m = \sum_{k \in \mathbb{Z}_{m+1}} \frac{1}{k}\binom{m}{k-1}(n)^k H_{m+1-k}(n)$,

where $H_k(n) = \prod_{p|n}(1 - p^{k-1})B_k \ \ (0 \leq i \leq m)$.

The next theorem takes advantage of these equalities.

Conjecture 3.2 (Agoh's Conjecture) *$n \in \mathbb{P}$ if and only if $nB_{n-1} \equiv -1 \pmod{n}$.*

Theorem 3.20 *Agoh's conjecture is equivalent to Giuga's conjecture.*

Proof: (Agoh) Suppose that n is prime. Then by the von Staudt-Clausen Theorem,

$$nB_{n-1} = n(A_{n-1} - \sum_{p-1|n-1} \frac{1}{p}) \equiv -1 \pmod{n}.$$

Therefore, assume n is composite. Then

$$\sum_{k \in \mathbb{Z}_{n-1}} k^{n-1} = \sum_{k \in \mathbb{Z}_n} \frac{1}{k} \binom{n-1}{k-1} n^k B_{n-k}.$$

Notice that if $p-1|n-1$, nB_{n-1} is invertible modulo p. Further, if $p-1 \not| n-1$, nB_{n-1} is invertible modulo p. Hence nB_{n-k}, $k \geq 3$, is invertible modulo p for any prime factor p of n. Also, $nB_{n-2} = 0$ as n is odd. It is therefore clear that

$$\sum_{k \in \mathbb{Z}_n} \frac{1}{k} \binom{n-1}{k-1} n^k B_{n-k} \equiv nB_{n-1} \pmod{n}.$$

■

In his paper, Agoh proved some important congruences involving Bernoulli numbers modulo prime powers [2].

Proposition 3.5 *Take $n \in \Sigma$. Then for any prime factor p of n:*

(i) $pB_{n-p} \equiv p-1 \pmod{p^3}$,

(ii) $pB_{(n/p)-1} \equiv p-1 \pmod{p^2}$,

(iii) $pB_{((n/p)-1)/p} \equiv p-1 \pmod{p}$.

Proof: Recall:

$$\sum_{k \in \mathbb{Z}_{n-1}} k^{n-1} = \sum_{k \in \mathbb{Z}_n} \frac{1}{k} \binom{n-1}{k-1} n^k B_{n-k}.$$

Now, it is immediate from Corollary 3.2 on page 39 that for $n \in \Sigma$ and any a with $p \nmid a$ that $a^{n-p} \equiv 1 \pmod{p^3}$. Hence, we have

$$\sum_{k \in \mathbb{Z}_n} \frac{1}{k}\binom{n-1}{k-1} n^k B_{n-k} \equiv p - 1 \pmod{p^3}.$$

Clearly, however, $B_{n-p-1} = 0$ and when $k \geq 3$,

$$\frac{1}{k}\binom{n-1}{k-1} n^k B_{n-k} \equiv 0 \pmod{p^3},$$

by the von Staudt-Clausen theorem. Thus, it must be the term pB_{n-p} that is congruent to $p - 1 \pmod{p^3}$. Parts (ii) and (iii) can be found with a similar process.

■

We can now add to our knowledge of Giuga sequences. Define Λ to be any subset of the set of prime factors p of a fixed $n \in \Sigma$. The next result (due to Agoh) follows without a large amount of work.

Theorem 3.21 *Let $M = M(\Lambda) = \prod_{p \in \Lambda} p$ and $t = t(\Lambda)$ be the number of elements in Λ. If $n \in \Sigma$, then*

$$\left(\sum_{p \in \Lambda} \frac{M}{p}\right)\left(\prod_{p \in \Lambda} \frac{1 - p^{n-2}}{1 - p}\right) \equiv (-1)^{t-1} \pmod{M}.$$

In particular,

$$\prod_{p \mid n} \frac{1 - p^{n-2}}{1 - p} \equiv (-1)^{s-1} \pmod{n},$$

where s is the number of prime factors of n.

Proof: Since $n \in \Sigma$, it must be the case that $(p-1)|(n-1)$ for all $p \in \Lambda$. From the von Staudt-Clausen Theorem (Theorem 2.10), we have

$$MB_{n-1} \equiv -M \sum_{p \in \Lambda} \frac{1}{p} \pmod{M}.$$

Recall also that

$$\sum_{k\in \mathbb{Z}_M^*} k^{n-1} = \sum_{k\in \mathbb{Z}_M} \frac{1}{k}\binom{n-1}{k-1} M^k H_{n-k}(M).$$

Since this sum is congruent to $\phi(M) \pmod{M}$, and

$$\frac{1}{k}\binom{n-1}{k-1} M^{k-1} \equiv 0 \pmod{M},$$

for $k \geq 2$, it follows that

$$\phi(M) \equiv MH_{n-1}(M) \equiv -\left(\prod_{p\in\Lambda}(1-p^{n-2})\right)\left(M\sum_{p\in\Lambda}\frac{1}{p}\right) \pmod{M},$$

which shows the first congruence (from Corollary 3.3 page 39). When $M = n$, the second result follows from the first with the use of Corollary 3.5. ∎

3.5.1 Giuga Quotients

If Giuga's conjecture is true, then like Wilson's theorem, it would be a useful number theoretic tool. Therefore, we shall continue studying Giuga's conjecture in the same way as Wilson's theorem. One particular aspect of Wilson's theorem that has been studied is what are known as Wilson quotients. This section will discuss Giuga quotients and other related quotient values. These results are due to Agoh and can be found in his paper "On Giuga's Conjecture" [2].

Definition 3.9 *Define the following four quotients:*

(I) $q_p(a) = \frac{a^{p-1}-1}{p}$ $(p \nmid a)$, *the Fermat Quotient of* p.

(II) $q(a,n) = \frac{a^{\phi(n)}-1}{n}$ $((a,n)=1)$, *the Euler Quotient of* n.

(III) $C(a,n) = \frac{a^{n-1}-1}{n}$ $(n \in \Gamma,\ (a,n)=1)$, *the Carmichael Quotient of* n.

(IV) $G_p(a,n) = \frac{a^{n-p}-1}{p^3}$ $(n \in \Sigma,\ p|n,\ p \nmid a)$, *the Giuga Quotient of* n.

Proposition 3.6 *With a, p and n and b as allowable values from Definition 3.9,*

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$$

$$q(ab, n) \equiv q(a, n) + q(b, n) \pmod{n}$$

$$C(ab, n) \equiv C(a, n) + C(b, n) \pmod{n}$$

$$G_p(ab, n) \equiv G_p(a, n) + G_p(b, n) \pmod{p^3}.$$

It can further be shown [2] that Giuga's conjecture is equivalent to saying $G_p(a, n) = 0$ for all bases a with $p \not| a$.

Before we proceed to derive properties pertaining to Giuga quotients, we require some background. The first result is due to Lerch [26].

Proposition 3.7 *If $n \geq 2$ and a are integers with $(a, n) = 1$, then*

$$q(a, n) \equiv \sum_{\substack{k \leq n-1 \\ (k,n)=1}} \frac{1}{ak} \left\lfloor \frac{ak}{n} \right\rfloor \pmod{n}.$$

Further, if p is prime and $p \not| a$, then

$$q_p(a) \equiv \sum_{k=1}^{p-1} \frac{1}{ak} \left\lfloor \frac{ak}{p} \right\rfloor \pmod{p}.$$

Wilson's theorem states

$$n \text{ is prime } \Leftrightarrow (n-1)! \equiv -1 \pmod{n}.$$

From this, we define, in the obvious way, a Wilson quotient.

Definition 3.10 *Take $m \geq 2$. Define*

$$J(m) = \prod_{\substack{j < m \\ (j,m)=1}} j.$$

Further, define

$$\varepsilon_m = \begin{cases} -1 & \text{when } q \text{ odd and } m = 2, 4, q^\alpha, 2q^\alpha \\ 1 & \text{Otherwise} \end{cases}.$$

Then denote:

(V) $W_p = \frac{(p-1)!+1}{p}$ *(p is prime), the Wilson Quotient of p,*

(VI) $W(m) = \frac{J(m)-\varepsilon_m}{m}$, *the Generalized Wilson Quotient of m.*

As is the case with the previous four quotients, (V) and (VI) are both integers and can be shown to have the following congruences hold. The proofs of these can be found in [3].

Proposition 3.8

$$\varepsilon_m \phi(m) W(m) \equiv \sum_{\substack{a \le m-1 \\ (a,m)=1}} q(a,m) \pmod{m}.$$

and if p is an odd prime,

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}.$$

Proposition 3.9 (Voronoi's Congruence) *Let* $t \ge 1$, $m \ge 2$ *and a be integers with* $(a, m) = 1$. *Then,*

$$\frac{(a^t - 1)\sum_{i=1}^{t+1} \frac{1}{i}\binom{t}{i-1} m^i H_{t+1-i}(m)}{m} \equiv t \sum_{\substack{k \le m-1 \\ (k,m)=1}} (ak)^{t-1} \left\lfloor \frac{ak}{m} \right\rfloor \pmod{m}.$$

Now, by using the above tools, we can make the following two assertions about Carmichael and Giuga quotients.

Proposition 3.10 *If* $n \in \Gamma$ *and* $(a, n) = 1$, *then*

$$\phi(n) C(a,n) \equiv (n-1) q(a,n) \pmod{n}.$$

Also, if $n \in \Sigma$, $p|n$ *and* $p \not| a$, *then*

$$(p-1)G_p(a,n) \equiv \frac{n-p}{p^2} q_p(a) \pmod{p}.$$

Proof: Take $m = n$ and $t = n-1$ in Proposition 3.9. Then

$$C(a,n) \sum_{i=1}^{n} \frac{1}{i} \binom{n-1}{i-1} n^i H_{n-i}(n) \equiv (n-1) \sum_{\substack{k \le m-1 \\ (k,m)=1}} (ak)^{n-2} \left\lfloor \frac{ak}{n} \right\rfloor \pmod{n}.$$

Since $n \in \Gamma$,

$$\sum_{i=1}^{n} \frac{1}{i} \binom{n-1}{i-1} n^i H_{n-i}(n) \equiv \phi(n) \pmod{n},$$

and

$$(ak)^{n-2} \equiv \frac{1}{ak} \pmod{n}.$$

The result now follows from Proposition 3.7.

In a similar way, take $m = p^3$ and $t = n-p$ in Proposition 3.9, then

$$G_p(a,n) \sum_{i=1}^{n-p+1} \frac{1}{i} \binom{n-p}{i-1} (p^3)^i H_{n-p+1-i}(p^3)$$
$$\equiv (n-p) \sum_{\substack{k \le p^3-1 \\ (k,p)=1}} (ak)^{n-p-1} \left\lfloor \frac{ak}{p^3} \right\rfloor \pmod{p^3}.$$

Since, $n \in \Sigma$, we have

$$\sum_{i=1}^{n-p+1} \frac{1}{i} \binom{n-p}{i-1} (p^3)^i H_{n-p+1-i}(p^3) \equiv p^2(p-1) \pmod{p^3}.$$

Hence,

$$(ak)^{n-p-1} \equiv \frac{1}{ak} \pmod{p^3}.$$

Now, by Proposition 3.7, this implies that

$$(p-1)G_p(a,n) \equiv \frac{n-p}{p^2} q(a,p^3) \pmod{p}.$$

If $q(a,p^3) \equiv q_p(a) \pmod{p}$, we are done. To verify this, note that since p is odd,

$$\binom{p^2}{i} p^{i-3} \equiv 0 \pmod{p}$$

for every $i \geq 2$. It follows that

$$\begin{aligned} q(a,p^3) &= \frac{a^{\phi(p^3)} - 1}{p^3} \\ &= \frac{1}{p^3} \sum_{i=1}^{p^2} \binom{p^2}{i} (a^{p-1} - 1)^i \\ &= \sum_{i=1}^{p^2} \binom{p^2}{i} p^{i-3} (q_p(a))^i \\ &\equiv q_p(a) \pmod{p}, \end{aligned}$$

hence showing all of the required elements. ∎

Corollary 3.15 *If $n \in \Gamma$, then*

$$\sum_{\substack{a \leq n-1 \\ (a,n)=1}} C(a,n) \equiv -\varepsilon_n W(n) \pmod{n}.$$

Also, if $n \in \Sigma$, then for any prime factor p of n,

$$\sum_{a=1}^{p-1} G_p(a,n) \equiv -\frac{n-p}{p^2} W_p \pmod{p}.$$

Proof: The results follow almost immediately from Proposition 3.8 and Proposition 3.10. ∎

3.6 Open Problems

The following is a list of open problems, some of which are mentioned in [8] and [2].

1. Is Giuga's conjecture true?

2. Is Agoh's conjecture true?

3. Is it possible to deduce properties about Giuga numbers and Carmichael numbers from Euler numbers?

4. Is it possible to show that no Giuga number can also be a Carmichael number?

5. Can one show that no Carmichael sequence can also be a Giuga sequence?

6. Does every Giuga sequence contain factors p and q such that $p|q-1$ (if yes, then Giuga's conjecture is proved)?

7. Is there a Giuga sequence with only odd factors?

8. Are there infinitely many proper Giuga sequences?

9. Find a fast way to compute all Giuga sequences of a prescribed length.

10. Are there Giuga sequences with sum minus product value greater than 1?

11. Are there two distinct Giuga sequences whose product is the same?

12. Can each integer be an element of a Giuga sequence? If this were so, then the previous question is answered positively.

13. Show that $r_m(L_m) = i_m$ for $m = 5, \ldots, 27692$. This shows that a counterexample to Giuga's Conjecture must have over 36,069 digits.

14. Is there an analogous chart to the "Eightfold Way" using Agoh's conjecture?

15. Is there a practical way to use Giuga's conjecture in a cryptographic application sense?

16. Is there an equivalent conjecture to Giuga's using the Zeta function?

17. Is there an equivalent conjecture to Giuga's using Euler polynomials?

18. Is it possible to deduce Giuga or Carmichael number properties using Euler polynomials and the Riemann Zeta function?

4 Conclusion

Clearly there has been a shift, in the past 40 years, from the study of number theory for it's own intrinsic and theoretical value to more practical applications such as cryptography. It is time, however, to revert back to theoretical results which may or may not have significant practical applications.

Giuga's conjecture,

$$n \text{ is prime } \iff \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n},$$

is one of the many important theoretical results which are seemingly useless from a cryptographic point of view. Giuga's result is equivalent to Agoh's conjecture,

$$n \text{ is prime } \iff nB_n \equiv -1 \pmod{n}.$$

Due to poor algorithms for repeated exponentiations and finding Bernoulli numbers, neither of these conjectures has been used in practical applications.

The most important result of this thesis is a complete compilation of all of the work done in the area of Giuga's conjecture. Nearly 55 years of work has been collected and placed in one document as a reference for future work. For a compact list of results, the reader is directed to Appendix 1.

Lastly, I will conclude with a word to future researchers in this area. Giuga's conjecture is as strange and complicated as anything in mathematics. To get a good handle on it or to even have a remote possibility of proving it, future work will have to center around the Carmichael condition and properties of Carmichael numbers. Induction style proofs of Giuga's conjecture seem impossible. Hence, proving that no Giuga number could also be a Carmichael number appears to be the most fruitful method for future work. For a detailed list of unsolved problems surrounding Giuga's

conjecture, please see Section 3.6. Any progress on any of the problems would be of great help to those of us on a quest to prove the conjecture.

Appendix 1: Giuga's Conjecture Results

For quick reference, the following is a compilation of all results related directly to Giuga's conjecture. The table continues on subsequent pages.

Result	Document Reference	Due To
$n \in \Sigma$ if and only if for each prime divisor p of n we have $(p-1) \mid ((n/p)-1)$ and $p \mid ((n/p)-1)$.	Theorem 3.1	Borwein
$n \in \Sigma \Rightarrow n$ is square-free.	Corollary 3.1	Borwein
$n \in \Sigma$ if and only if $p^2(p-1) \mid (n-p)$ for any prime divisor p of n.	Corollary 3.2	Agoh
If $n \in \Sigma$, then $(\phi(n), n) = 1$.	Corollary 3.3	Agoh
$n \in \Sigma$ and is composite if and only if $n \in \Gamma$ and $n \in \mathcal{G}$.	Theorem 3.2	Borwein
A finite increasing sequence of integers $\{a_1, \ldots a_m\}$ satisfies $a_i \mid a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_m - 1$ for every $i \leq m$ if and only if it is a Giuga sequence.	Theorem 3.3	Borwein
n is a Giuga number if and only if $\sum_{p\mid n} \frac{1}{p} - \prod_{p\mid n} \frac{1}{p} \in \mathbb{N}$.	Corollary 3.4	Borwein
$n \in \Sigma$ if for any prime factor p of n $n \sum_{p\mid n} \frac{1}{p} \equiv 1 \pmod{n}$.	Corollary 3.5	Agoh

Table 11: Giuga's Conjecture Results

Result	Document Reference	Due To
Let m be a fixed natural number. Then there exist only finitely many Giuga sequences of length m.	Proposition 3.1	Buck, Hobart
Define $\mathcal{G}_m =$ $\{a \in \mathbb{N} \mid a$ is an element of a Giuga sequence of length $m\}$ Then, for any fixed $m \in \mathbb{N}$, $\mathcal{G}_m$ has a maximal element.	Corollary 3.6	Buck, Hobart
If $\{a_1, a_2, \ldots, a_m\}$ is a Giuga sequence with sum minus product x, then $m > a_1 x$.	Corollary 3.2	Buck, Hobart
Let m be a fixed natural number and suppose that $\{a_1, \ldots a_m\}$ is a Giuga sequence. Then for any j such that $a_1 + 1 - j > 0$, $a_j < \frac{a_1(m-j+1)}{a_1-j+1}$.	Theorem 3.4	Buck, Hobart
Suppose $P = \{p_1, p_2 \ldots p_m\}$ is a normal family of primes and let $n = p_1 p_2 \cdots p_m$. Then there is a unique group of order n up to isomorphism.	Theorem 3.12	Wong
If n is divisible by primes p_i, p_j for which $p_i \mid p_j - 1$, then there exists a non-cyclic group of order n. Note: p_i and p_j need not be distinct, thus n is necessarily square-free.	Theorem 3.13	Wong
Let $P = \{p_1, p_2, \ldots, p_l\}$ be a normal family of primes, and define $r_i = \text{lcm}_{i \neq j}(p_j)$. Then any number of the form $p_1^{k_1 r_1} p_2^{k_2 r_2} \cdots p_l^{k_l r_l}$ with $k \in \mathbb{Z}^+$ is pseudo-Carmichael. Conversely, if n is pseudo-Carmichael, then its prime factors form a normal family.	Theorem 3.14	Wong

<table>
<tr><th colspan="6">Result</th><th>Document Reference</th><th>Due To</th></tr>
<tr><td colspan="6">n is co-Giuga if and only if
$$\prod_{p|n}\left(\frac{1}{p}-1\right)-\sum_{p|n}\left(1-\frac{1}{p}\right)\in\mathbb{Z}.$$</td><td>Theorem 3.15</td><td>Wong</td></tr>
<tr><td colspan="6">There are no non-trivial co-Giuga numbers with fewer than 7695 prime factors.</td><td>Theorem 3.16</td><td>Wong</td></tr>
<tr><td>I</td><td>r</td><td>m</td><td>Conditions on n</td><td>Trivial cases</td><td>Non-Trivial examples</td><td>Cor.</td></tr>
<tr><td>$\mathbb{Z}_n$</td><td>$n-1$</td><td>$\phi(n)$</td><td>Giuga</td><td>Primes</td><td>30, 858, 1722, etc.</td><td>3.7</td></tr>
<tr><td>$\mathbb{Z}_n$</td><td>$n-1$</td><td>$n-1$</td><td>Giuga and Carmichael</td><td>None</td><td>$>13,800$ digits</td><td>3.8</td></tr>
<tr><td>$\mathbb{Z}_n$</td><td>$\phi(n)$</td><td>$\phi(n)$</td><td>Co-Giuga</td><td>Prime powers</td><td>>7694 Prime Factors</td><td>3.9</td></tr>
<tr><td>$\mathbb{Z}_n$</td><td>$\phi(n)$</td><td>$n-1$</td><td>Odd, Co-Giuga and Pseudo-Carmichael</td><td>Odd Prime Powers</td><td>>7694 Prime Factors</td><td>3.10</td></tr>
<tr><td>$\mathbb{Z}_n^*$</td><td>$n-1$</td><td>$\phi(n)$</td><td>Prime</td><td>Primes</td><td>None</td><td>3.11</td></tr>
<tr><td>$\mathbb{Z}_n^*$</td><td>$n-1$</td><td>$n-1$</td><td>Prime</td><td>Primes</td><td>None</td><td>3.12</td></tr>
<tr><td>$\mathbb{Z}_n^*$</td><td>$\phi(n)$</td><td>$\phi(n)$</td><td>All $n\in\mathbb{N}$</td><td>All $n\in\mathbb{N}$</td><td>None</td><td>3.13</td></tr>
<tr><td>$\mathbb{Z}_n^*$</td><td>$\phi(n)$</td><td>$n-1$</td><td>Odd and Pseudo-Carmichael</td><td>Odd Prime Powers</td><td>Carmichael Numbers, 45, 225, 325, ...</td><td>3.14</td></tr>
<tr><td colspan="6"></td><td>Table 10</td><td>Wong</td></tr>
</table>

Result	Document Reference	Due To
Take an initial sequence of length $m-2$. Let $A = \{a_1, a_2, \ldots, a_{m-2}\}$ be such a sequence. Let $$P = a_1 a_2 \cdots a_{m-2}, \quad S = \frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_{m-2}}.$$ Fix an integer $v > S$. Take any integers x, y with $x \cdot y = P(P+S-v)$ and $y > x$. Let $$a_{m-1} = \frac{P+x}{P(v-S)}, \quad a_m = \frac{P+y}{P(v-S)}.$$ Then, $$S + \frac{1}{a_{m-1}} + \frac{1}{a_m} - \frac{1}{P n_{m-1} n_m} = v.$$ Hence, $A \cup \{a_{m-1}, a_m\} = \{a_1, a_2, \ldots, a_{m-2}, a_{m-1}, a_m\}$ is a Giuga sequence if and only if $a_{m-1} \in \mathbb{N}$.	Theorem 3.17	Borwein
Let $n = p_1 p_2 \cdots p_m$ be an odd Giuga number. Then, $n - v \equiv 1 \pmod 4$.	Proposition 3.4	Borwein
Take a Giuga sequence of length m, which satisfies $a_m = a_1 \cdots a_{m-1} - 1$. Then, let $$\widetilde{a}_m = a_1 \cdots a_{m-1} + 1, \quad a_{m+1} = a_1 \cdots a_{m-1} \widetilde{a}_m - 1.$$ Then, $\{a_1, \ldots, a_{m-1}, \widetilde{a}_m, \widetilde{a}_{m+1}\}$ is a Giuga sequence with the same sum minus product value.	Theorem 3.19	Borwein
(Agoh's Conjecture) $n \in \Sigma$ if and only if $nB_{n-1} \equiv -1 \pmod n$.	Theorem 3.2	Agoh
Take $n \in \Sigma$, then for any prime factor p of n: (i) $pB_{n-p} \equiv p-1 \pmod{p^3}$, (ii) $pB_{(n/p)-1} \equiv p-1 \pmod{p^2}$, (iii) $pB_{((n/p)-1)/p} \equiv p-1 \pmod p$.	Proposition 3.5	Agoh

Result	Document Reference	Due To
Let $M = M(\Lambda) = \prod_{p\in\Lambda} p$ and $t = t(\Lambda)$ be the number of elements in Λ. If $n \in \Sigma$, then $$\left(\sum_{p\in\Lambda} \frac{M}{p}\right)\left(\prod_{p\in\Lambda} \frac{1-p^{n-2}}{1-p}\right) \equiv (-1)^{t-1} \pmod{M}.$$ In particular, $$\prod_{p\mid n} \frac{1-p^{n-2}}{1-p} \equiv (-1)^{s-1} \pmod{n},$$ where s is the number of prime factors of n.	Theorem 3.21	Agoh

Appendix 2: Modern Primality Tests

	Name	Theory	Ref.	Algorithm
1.	AKS Test	p prime $\Leftrightarrow$ $(x-a)^p \equiv (x^p - a) \pmod{p}$	[4]	$(x-a)^N \equiv (x^N - a) \pmod{x^r - 1, N}$ implies N prime.
2.	Pépin Test	Pépin's Theorem	[37]	Take $n \geq 2$ and $k \geq 3$ $k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then $\Leftrightarrow \left(\frac{k}{F_n}\right) = -1$ and F_n is prime.
3.	Pocklington Test	Pocklington's Theorem	[11]	Let p be an odd prime and select k so that $1 \leq k \leq 2(p+1)$ and $p \nmid k$. Set $N = 2kp + 1$. Then, N is prime iff $\gcd(a^k + 1, N) = 1$.
4.	Proth Test	Proth's Theorem	[36]	$N = k \cdot 2^n + 1$, with $k < 2^n$ odd, is prime if there is an integer a such that $a^{(N-1)/2} \equiv -1 \pmod{N}$
5.	Selfridge-Hurwitz Residue Test	Pépin's Theorem	[54]	Let $R_n \equiv 3^{(F_n-1)/2} \pmod{F_n}$. F_n is composite, $n > 5$, if $R_n \pmod{2^{36}}$ doesn't vanish.
6.	Ward's Primality Test	Lucas Sequences	[37],	Take N odd and assume there is a Lucas sequence $\{U_n\}$ with associated Sylvester cyclotomic numbers $\{Q_n\}$ such that there is an $n > \sqrt{N}$, $(N, n) = 1$, for which $N \mid Q_n$. Then, N is prime unless it has one of the following forms $N = (n-1)^2$, with $n-1$ prime and $n > 4$, or $N = n^2 - 1$, with $n-1$ and $n+1$ prime.
7.	Wilson's Test	Wilson's Theorem	[36]	N is prime iff $(N-1)! \equiv -1 \pmod{N}$.

Table 12: Modern Prime Tests

	Name	Theory	Ref.	Algorithm
8.	Prime Diophantine Equations	Diophantine Equations	[52]	$k+2$ is prime iff there is a solution in $\mathbb{Z}^+$ to the following system: $wz+h+j-q=0$ $(gk+2g+k+1)(h+j)+h-z=0$ $16(k+1)^3(k+2)(n+1)^2+1-f^2=0$ $2n+p+1+z-e=0$ $e^3(e+2)(a+1)+1-o^2=0$ $(a^2-1)y^2+1-x^2=0$ $16r^2y^4(a^2-1)+1-u^2=0$ $n+l+v-y=0$ $(a^2-1)l^2+1-m^2=0$ $ai+k+1-l-i=0$ $\{[a+u^2(u^2-1)]^2-1\}(n+4dy)^2+1$ $-(x+cu)^2=0$ $b(2an+2a-n^2-2n-2)-m+p+$ $l(a-n-1)=0$ $s(2ap+2a-p^2-2p-2)-x+q+$ $y(a-p-1)=0$ $z+pl(a-p)+t(2ap-p^2-1)-$ $pm=0$
9.	Lucas-Lehmer Test	Lucas Sequences	[11]	Let $N+1=\prod_{j=1}^{n} q_j^{\beta_j}$ with q_j are prime factors and β_j their respective powers. If there exists a Lucas sequence U_ν such that $\gcd(U_{(N=1)/q_j}, N)=1\ \forall\ j=1\ldots n$ and $U_{N+1}\equiv 0 \pmod N$, then N is prime.

	Name	Theory	Ref.	Algorithm
10.	Frobenius Test	Ring Theory	[37]	Select $\left(\frac{b^2+4c}{N}\right) = -1$ and $\left(\frac{-c}{N}\right) = 1$. If $x^{(N+1)/2} \pmod{(n, x^2 - bx - c)} \in \mathbb{Z}/N\mathbb{Z}$, $x^{(N+1)} \pmod{(N, x^2-bx-c)} \equiv -c$, if $N^2 - 1 = 2^r s$ where s odd, and $x^s \equiv 1 \pmod{n, x^2-bx-c}$ and $x^{2^j s} \equiv -1 \pmod{n, x^2-bx-c} \forall j < r-1$, then N is a probable prime.
11.	AGKM Certificate	Elliptic Curves; Goldwasser and Kilian Theorem	[45]	The certificate consists of a list of 1. A point on an elliptic curve C: $y^2 = x^3 + g_2 x + g_3 \pmod{N}$ for some numbers g_2 and g_3. 2. A prime q with $q > (N^{1/4} + 1)^2$ such that for some other number k and $m = kq$ with $k \neq 1$, $mC(x, y, g_2, g_3, N)$ is the identity of the curve, but $kC(x, y, g_2, g_3, N)$ is not. Then N is prime.
12.	Pratt Certificate	Fermat's Little Theorem Converse	[11]	Take $N \in \mathbb{Z}^+$ and $\{P_i\}$ the set of prime factors of $N - 1$. Suppose there exists $x \in \mathbb{Z}^+$ such that $x^{N-1} \equiv 1 \pmod{N}$, but $x^e \not\equiv 1 \pmod{n}$ whenever e is one of $(n-1)/p_i$. Then N is prime.

	Name	Theory	Ref.	Algorithm
1.	Euler Test	Euler's Criterion	[25]	If N is prime, then $a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}$ where $(a\|p)$ is the Legendre symbol (the converse need not hold).
2.	Fermat Test	Fermat's Little Theorem	[13]	Select $a \in \mathbb{Z}^+$ then if N is prime $a^{N-1} \equiv 1 \pmod{N}$ (the converse need not hold).
3.	Miller's Test	Fermat's Little Theorem	[51]	Assume the extended Riemann hypothesis is true, then if N is an a-SPSP for all integers a with $1 < a < 2(\log n)2$, then N is prime
4.	Baillie-PSW Primality Test	Strong psp; Lucas psp	[31]	1. Perform a base 2 psp test on N. 2. Given the sequence $5, -7, 9, -11, 13, \ldots$, find the first number D for which $\left(\frac{D}{N}\right) = -1$. Then perform a Lucas PSP test with discriminant D on N. If N passes both tests, N is a probable prime.
5.	Rabin-Miller Test	Strong PSP	[13]	Given $N = 2^r s + 1$ with s odd, chose $a < N-1$. If $a^s \equiv 1 \pmod{n}$ or $a^{2^j s} \equiv -1 \pmod{n}$ for some $j \leq r-1$. Then, N is probably prime.

Table 13: Modern Pseudo-prime Tests

	Name	Theory	Ref.	Algorithm
1.	Giuga's Conjecture	Fermat's Little Theorem	[8]	$\sum_{k=1}^{N-1} \equiv -1 \pmod{N} \Leftrightarrow N$ is prime
2.	Agoh Conjecture	Bernoulli Numbers	[8]	$NB_{N-1} \equiv -1 \pmod{N} \Leftrightarrow N$ is prime
3.	Agoh-Giuga Conjecture	Equivalence of Giuga and Agoh Conjectures	[23]	$\sum_{p\|N,\ (p-1)\|(N-1)} \frac{N}{p} \equiv 1 \pmod{N} \Leftrightarrow N$ is prime.
4.	Feit-Thompson Conjecture	Feit-Thompson Theorem	[44]	For no primes $p, q > 400,000$ do $(p^q - 1)/(p-1)$ and $(q^p - 1)/(q-1)$ have a common factor.

Table 14: Prime Number Conjectures

	Name	Ref.	Algorithm
1.	Eratosthenes	[11]	Begin with a list of numbers up to N. Begin by crossing off all multiples of 2 that are larger than 2. Next move to the next number that is not crossed off. Cross off all multiples of that number but greater than it, that are not crossed off. Repeat this until you reach $\lfloor\sqrt{N}\rfloor$. The remaining numbers are prime.
2.	Number Field Sieve	[29]	Chose $r, e, s \in \mathbb{Z}$. Let $n = r^e - s$, where s is small. Now, select an extension degree $d \in \mathbb{Z}^+$. Given d, we proceed by selecting $k \in \mathbb{Z}^+$ (the smallest integer) such that $kd \geq e$, so that $r^{kd} \equiv sr^{kd-e} \pmod{n}$. Now, let $f(X) = X^d - c \in Z[X]$. Now, for a reasonable choice of d, any factor of f is also a nontrivial factor of n. So, assume that f is irreducible. So, we can now define a number field $\mathbb{Q}(\alpha)$ where α satisfies $f(\alpha) = 0$. We let Φ denote the ring homomorphism from $\mathbb{Z}[\alpha]$ to $\mathbb{Z}/n\mathbb{Z}$ that sends α to $m \pmod{n}$. The idea is to look at pairs of small co-prime integers a, b such that both $a + \alpha b$ and $a + mb$ are smooth. Because $\Phi(a + \alpha b) = (a + mb \pmod{n})$, each pair provides a congruence modulo n between two products. With enough of these pairs, we can then find a solution to $y^2 \equiv z^2 \pmod{n}$, and solve by the same method as the Quadratic Sieve.

Table 15: Modern Sieving Methods

	Name	Ref.	Algorithm
3.	Quadratic Sieve	[15]	The Quadratic Sieve attempts to find a solution to the congruence $x^2 \equiv y^2 \pmod{n}$ when $x \not\equiv \pm y \pmod{n}$, $x, y \in \mathbb{Z}$. From this, it follows that $n \mid (x-y)(x+y)$ but n divides neither $(x-y)$ nor $(x+y)$. So, $\gcd(n, x-y)$ and $\gcd(n, x+y)$ is a proper divisor of n. The QS finds relationships of the form $z_i^2 \equiv q_i \pmod{n}$, where the prime factorization of q_i is known. The set of divisors of q_i is known as the factor base (FB). When there are more primes than there are in the factor base, we can use algebra over the field GF(2). We combine the q_i's so that they form a square. This gives rise to $x^2 \equiv y^2 \pmod{n}$ where $x^2 = \prod z_i$ for the right z_i's.
4.	Multi-polynomial Quadratic Sieve	[15]	We try to solve the congruence $U_i^2 \equiv V_i^2 W_i \pmod{N}$, where W is easier to factor than N. Let $U(x) = a^2x + b$, $V = a$, and $W(x) = a^2x^2 + 2bx + c$ with $x \in [-M, M)$ where a, b and c satisfy the following relationship: $a^2 \approx \sqrt{2N}/M$, $b^2 - N = a^2c$, and $\lvert b \rvert < a^2/2$, and m is some fixed integer. So, we solve $U(x)^2 \equiv V^2 W(x) \pmod{N}$. Now, since W takes on its extreme values at $x = 0, \pm M$, and we can see that $\lvert W(0) \rvert \approx \lvert W(\pm M) \rvert \approx M\sqrt{N/2}$ and if $M \ll N$, we see $\lvert W(x) \rvert \ll N$ which implies that W is easier to factor. Also, since it is a quadratic polynomial, we know that if $d \mid W(x_0)$, for some x_0, then $d \mid x_0 + kd$, $\forall\, k$.

	Name	Ref.	Algorithm
1.	Aurifeuillean Factorization Method	[12]	A factorization of the form: $2^{4n+1}+1 = (2^{2n+1} - 2^{n+1}+1)(2^{2n+1}+2^{n+1}+1)$
2.	Brent's Factorization Method	[10]	A speed up algorithm applied to the second step of the Pollard algorithm. The algorithm provides a 24 % speed up factor over Pollard's original algorithm, however, provides no new insights into factoring.
3.	Continued Fraction Factorization	[25]	Begin by setting $b_{-1}1$, $b_0 = a_0 = \sqrt{n}$, and $x_0 = \sqrt{n} - a_0$. 1. Now, set $a_i = 1/x_{i-1}$ and then $x_i = 1/(x_{i-1} - a_i)$. 2. Next, set $b_i = a_i b_{i-1} + b_{i-2} \pmod{n}$. 3. Finally, compute $b_i^2 \pmod{n}$. Once this is done for several i's, factor the remainders and create a factor base $\mathcal{B}$. This gives rise to a method of creating the equation $x^2 \equiv y^2 \pmod{n}$ which we can factor so long as $x \neq \pm y$.
4.	Direct Search Factorization	[11]	A simple factorization method which consists of searching for factors of a number by systematically performing trial divisions.
5.	Euler's Factorization Method	[48]	Let $N = a^2 + b^2 = c^2 + d^2$. Then, $a^2 - c^2 = d^2 - b^2 = (a-c)(a+c) = (d-b)(d+b)$. If $k = \gcd(a-c),(d-b)$, then $a - c = kl$, $d - b = km$, and $\gcd l, m = 1$. Thus, $l(a+c) = m(d+b)$. Since $\gcd l, m = 1$, $m \mid a+c$ and $a + c = mn$, which gives $b + d = ln$. Therefore, $N = 1/4(2N + 2N) = 1/4(2a^2+2b^2+2c^2+2d^2) = 1/4[(d-b)^2+(a-c)^2+(a+c)^2+(d+b)^2] = 1/4[(kn)^2+(lk)^2+(nm)^2+(nl)^2] = 1/4(k^2+n^2)(l^2+m^2) = [(1/2k)^2+(1/2n)^2](l^2+m^2)$
6.	Excludent Factorization Method	[49]	A modification of the $x^2 \equiv y^2 \pmod{n}$ algorithms where we find $x^2 \equiv y^2 - N \pmod{E}$ for various moduli E. This method works best when the factors of N are about the same size.

Table 16: Modern Factoring Techniques

	Name	Ref.	Algorithm
7.	Dixon's Factorization Method	[17]	We hope to find integers x and y such that $x^2 \equiv y^2 \pmod{n}$. If such integers are found, there is a 50 % chance that $\gcd(n, x-y)$ is a factor of n. Chose r_i such that $g(r_i) \equiv r_i^2 \pmod{n}$, and try to factor $g(r_i)$. Continue finding and factoring $g(r_i)$ until $N \equiv \pi d$ are found. Now for each $g(r_i)$ we have $g(r_i) = p_{1i}^{a_{1i}} p_{2i}^{a_{2i}} \cdots p_{Ni}^{a_{Ni}}$, and the exponent vector $\mathbf{v}(r_i) = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{N1} \end{pmatrix}$. Now, if a_{ki} are even for any k, then $g(r_i)$ is a square number and hence a solution. If not, we find linear combinations $\sum_i c_i \mathbf{v}(r_i)$ such that the elements are all even. i.e. $\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{pmatrix} = \mathbf{0}$ (mod 2). Since each a_{ij} is either 1 or 0 (mod 2) we can replace a_{ij} with $b_{ij} = \begin{cases} 1 & if 2 \mid a_{ij} \\ 0 & if a_{ij} is odd \end{cases}$. Then, Gaussian elimination can be used to solve $\mathbf{bc} = \mathbf{z}$ for $\mathbf{c}$ where $\mathbf{z} = 0 \pmod{2}$. Once $\mathbf{c}$ is known, we have $\prod_k g(r_k) \equiv \prod_{k, c_k = 1} r_k^2 \pmod{n}$. This has a 50% chance of yielding a nontrivial factor of n.
8.	Fermat's Factorization Method	[38]	Select integers x, y such that $x^2 - y^2 = N$. Then $N = (x-y)(x+y)$ which is a (possibly partial) factorization of N.
9.	Legendre's Factorization Method	[50]	A prime factorization algorithm in which a sequence of trial divisors is chosen using a quadratic sieve. By using quadratic residues of N, the quadratic residues of the factors can also be found.
10.	Pollard $p-1$ Factorization Method	[11]	A factorization method where if $p-1$ is dissolved into small primes by finding an m such that $m \equiv c^q \pmod{N}$ where $p-1 \mid q$ with q a large number and $\gcd(c, N) = 1$. Since $p-1 \mid q$, $m \equiv 1 \pmod{p}$, so $p \mid m-1$. There is therefore a good chance that $N \not\mid m-1$, in which case $\gcd(m-1, n)$ will be a nontrivial divisor of n.

	Name	Ref.	Algorithm
11.	Pollard Rho Factorization Method	[25]	The Pollard Rho Factorization method relies on iterating a formula until it falls into a cycle. Let $N = pq$ where p, q are unknown prime factors. Iterating through the formula $x_{n+1} \equiv x_n^2 + a \pmod{N}$ (or almost any other polynomial) for an initial value x_0 will produce a sequence of numbers that eventually fall into a cycle. Now, since $N = pq$ where $(p, q) = 1$, the CRT guarantees that each value of $x \pmod{N}$ corresponds to a uniquely determined pair of values $(x \pmod{p}, x \pmod{q})$. Also, the sequence of x_n follows the same formula modulo p and q. That is: $x_{n+1} = [x_n \pmod{p}]^2 + a \pmod{p}$ $x_{n+1} = [x_n \pmod{q}]^2 + a \pmod{q}$. Therefore, the sequence modulo p will fall into a shorter cycle of length on the order of $r(1) - 0$. It can be directly verified that two values x_1 and x_2 have the same value modulo p by computing $\gcd(\lvert x_2 - x_1 \rvert, n)$, which is equal to p.
12.	Williams $p+1$ Factorization Method	[56]	Uses the properties of the Lucas functions $U_n(P, 1)$ and $V_n(P, 1)$ to find a prime factor p of N when $p+1$ has only small factors and the Legendre symbol $(P^2 - 4/P) = -1$.

Appendix 3: Number Theoretic Congruences

Congruence	Reference
$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \frac{B_b}{b} \pmod{p} \; \forall \; k \in \mathbb{N}$	Kummer [35]
$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv k\frac{B_{p-1+b}}{p-1+b} - (k-1)(1-p^{b-1})\frac{B_b}{b} \pmod{p^2}$	Sun [42]
$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \binom{k}{2}\frac{B_{2(p-1)+b}}{2(p-1)+b} - k(k-2)\frac{B_{p-1+b}}{p-1+b} + \binom{k-1}{2}(1-p^{b-1})\frac{B_b}{b} \pmod{p^3}$	Sun [42]
$B_{p-3} \equiv \frac{-3}{p^2}(\sum_{i=1}^{n-1}\frac{1}{i})$	Sun [42]
$(p-1)! \equiv \frac{pB_{2p-2}}{2p-2} - \frac{pB_{p-1}}{p-1} - \frac{1}{2}(\frac{pB_{p-1}}{p-1})^2 \pmod{p^3}$	Sun [42]
$(p-1)! \equiv pB_{p-1} - p \pmod{p^2}$	Beeger [7]
$\sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv 0 \pmod{p^n} \quad b > n \;\; b \not\equiv 0 \pmod{p-1}$	Ireland and Rosen [22]
$\frac{B_k(x)-B_k(x_0)}{k} \equiv (x-x_0)B_{k-1} \pmod{p}$	Sun [42]
$(1-p^{k(p-1)+b-1})\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \sum_{r=0}^{n-1}(-1)^{n-1-r}\binom{k-1-r}{n-1-r}\binom{k}{r}$ $(1-p^{r(p-1)+b-1})\frac{B_{r(p-1)+b}}{r(p-1)+b} \pmod{p^n}$	Sun [42]

Table 17: Number Theoretic Congruences

Congruence	Reference
For $k \in \{1, 2, \ldots, p-4\}$, $$\sum_{x=1}^{p-1} x^{-k} \equiv \begin{cases} \frac{k(k-1)}{2} \frac{B_{p-2-k}}{p-2-k} p^2 \pmod{p^3} & \text{if } k \text{ is odd} \\ k(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k})p \pmod{p^3} & \text{if } k \text{ is odd} \end{cases}$$	Sun [42]
$\sum_{x=1}^{p-1} x^{-(p-3)} \equiv (\frac{1}{2} - 3B_{p+1})p - \frac{4}{3}p^2 \pmod{p^3}$	Sun [42]
$\sum_{x=1}^{p-1} x^{-(p-2)} \equiv -(2 - pB_{p-1})p - \frac{5}{2}p^2 \pmod{p^3}$	Sun [42]
$\sum_{x=1}^{p-1} x^{-(p-1)} \equiv pB_{2p-2} - 3pB_{p-1} + 3(p-1) \pmod{p^3}$	Sun [42]
Let $k < p$ then, $$\sum_{x=1}^{p-1} x^{-1} \equiv \begin{cases} \frac{k}{k+1} pB_{p-1-k} \pmod{p^2} & \text{if } k < p-1 \\ -pB_{p-1} + 2(p-1) \pmod{p^2} & \text{if } k = p-1 \end{cases}$$	Sun [2000]

Appendix 4: Algorithms

Giuga Sequences

Since we know that there are only finitely many Giuga sequences of a fixed length and we can bound each term, we have the following algorithm to compute Giuga sequences of a fixed length by brute force (Thanks to Jed Brown and Julian Buck (personal communications) for their help with the algorithm).

```
#include <stdio.h> #include <math.h>

const unsigned N = 6; const double omega = 1.0e12; const double
epsilon = 1e-13;

int g_count;

inline void printStack( unsigned * s, unsigned level, double sum,
double overShoot ); void next( unsigned [], double sum, unsigned
prod, unsigned level );

int main() {
    g_count=0;
    unsigned stack[10];
    stack[1] = 2;
    stack[2] = 3;
    double sum = 1.0/2.0 + 1.0/3.0;
    next( stack, sum, 6, 2 );

    printf( "count = %i\n", g_count );

    return 0;
}

inline void next( unsigned * s, double sum, unsigned prod,
unsigned level ) {
    double overShoot = sum-1-(1.0/prod);
    if ( overShoot > epsilon ) return;
    if ( sum > 1 ) {
    if ( overShoot > -epsilon )
        printStack(s,level,sum, overShoot);
    return;
    }
    if ( level == N ) return;
    double upperBound = ( (N - level)*prod ) / ( prod*(1.0-sum) );
    if ( upperBound > omega ) return;
    //printf( "Current Stack is: " );
    //printStack( s, level, sum, overShoot );
    //printf( "upper bound is: %f\n", upperBound );
    for ( unsigned i=s[level]+1 ; i < (unsigned)ceil( upperBound ) ; ++i ) {
    s[level+1] = i;
    next( s, sum+(1.0/i), prod*i, level+1 );
    }
```

```
}

inline void printStack( unsigned s[], unsigned level, double sum,
double overShoot ) {
    g_count++;
    for ( unsigned i=1 ; i<=level ; i++)
    printf( "%i  ", s[i] );
    printf( "  sum= %f  overShoot= %e \n", sum, overShoot );
}
```

Notational Conventions

Symbol	Definition
	Chapter 1
$\mathbb{N}$	Natural Numbers: $\{0, 1, 2, \ldots\}$
$\mathbb{Z}^+$	Positive Integers: $\{1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of Primes: $\{2, 3, 5, 7, 11, \ldots\}$
	Chapter 2
B_n	The n^{th} Bernoulli Number
$B_n(x)$	The n^{th} Bernoulli Polynomial
$denom(x)$	The denominator of x
E_n	The n^{th} Euler Number
$E_n(x)$	The n^{th} Euler Polynomial
$E_n(0)$	The Constant Term of n^{th} Euler Polynomial
$\zeta(n)$	The Riemann Zeta Function
	Chapter 3
Σ	$\{n \mid \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}\}$
Γ	The Set of Carmichael Numbers
$\mathcal{G}$	$\{n \mid p \mid (n/p - 1)\ \forall\ p \mid n\}$
$q_p(a)$	Fermat Quotient of p
$q(a, n)$	Euler Quotient of n
$C(a, n)$	Carmichael Quotient of n
$G_p(a, n)$	Giuga Quotient of n

Table 18: Notational Conventions

References

[1] M. Abramowitz, I. Stegun, *Handbook of Mathematical Functions*, Dover, New York, 9th edition, 1972.

[2] T. Agoh, "On Giuga's Conjecture", *Manuscripta Mathematica*, 87 (1995), 501 - 510.

[3] T. Agoh, K. Dilcher and L. Skula, "Wilson Quotients for Composite Moduli", *Math. Comput.* 67 (1981), 843-861.

[4] M. Agrawal, N. Kayal and N. Saxena, "Primes in P", *Preprint*, 2002. http://www.cse.iitk.ac.in/primality.pdf.

[5] W. Alford, A. Granville and C. Pomerance, "There are Infinitely Many Carmichael Numbers." *Ann. Math.* 140 (1994), 703-722.

[6] E. Bedocchi, "Nota ad una congettura sui numeri primi", *Riv. Mat. Univ. Parma* (1985), 11, 229-236.

[7] N. Beeger, "On some new congruences in the theory of Bernoulli numbers", *Bull. Amer. Math. Soc.*, 44 (1938), 684-688.

[8] D. Borwein, J. Borwein, P. Borwein and R. Girgensohn, "Giuga's Conjecture on Primality", *Amer. Math. Monthly* (1996), 103, 40-50.

[9] J. Borwein, D. Bradley,and R. Crandall "Computational strategies for the Riemann zeta function", *J. Comput. Appl. Math.* (2000), 121, 247-296.

[10] R. Brent. "An Improved Monte Carlo Factorization Algorithm", *Nordisk Tidskrift for Informationsbehandlung (BIT)* (1980), 20, 176-184.

[11] D. Bressoud, S. Wagon, *Computational Number Theory*, Key College Publishing, 1999.

[12] J. Brillhart, D. H. Lehmer, J. Selfridge, S. S. Wagstaff, and B. Tuckerman "Factorizations of , $b^n \pm 1, b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers", rev. ed. *Amer. Math. Soc.* Providence, Rhode Island (1988), 2nd edition.

[13] J. Buchmann, *Introduction to Cryptography*, Springer-Verlag, NY, 2000.

[14] R. Carmichael, "A Note on a New Number Theory Function." *Bull. Amer. Math. Soc.* (1910), 16, 232-238.

[15] Carrier, Wagstaff, "Implementing the Hypercube Quadratic Sieve with Two Large Primes" *Center for Education and Research in Information Assurance and Security*, 2003.

[16] R. Crandall, *Topics in Adanced Scientific Computation*, Springer-Verlag, New York. 1996.

[17] J. Dixon, "Asymptotically Fast Factorization of Integers", *Math. Comput.* (1981), 36, 255-260.

[18] H. Dubner, "Carmichael numbers of the form $(6k + 1)(12k + 1)(18k + 1)$" *Journal of Integer Sequences* (2002), 5.

[19] J. Gallian, *Contemporary Abstract Algebra*, Houghton Mifflin, Boston MA, 2002.

[20] G. Giuga, "Su una presumibile proprietá caratteristica dei numeri primi" *Ist. Lombardo Sci. Lett. Rend. A* (1950), 83:511-528.

[21] R. Guy, *Unsolved Problems in Number Theory*, New York, Springer-Verlag, 1996.

[22] K. Ireland, M. Rosen. *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1990.

[23] B. Kellner. "Über irreguläre Paare höherer Ordnungen", *Diplomarbeit. Math. Institut der Georg August Universität zu Göttingen* (2002). http://www.bernoulli.org/ bk/irrpairord.pdf.

[24] A. Klappenecker, "The AKS Primality Test; Results from Analytic Number Theory", (2002), NP.

[25] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

[26] M. Lerch, "Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$", *Math. Annalen* (1905), 60, 471-490.

[27] M. Morrison, J. Brillhart, "A Method of Factoring and the Factorization of F_7", *Math. Comput.* (1975), 29, 183-205.

[28] R. Pinch, "The Carmichael Numbers up to 10^{15}", *Math. Comput.*, 61 (1993), 381-391.

[29] J. M. Pollard, "A Monte Carlo Method for Factorization", *BIT*, 15 (1974), 331-334.

[30] J. M. Pollard, "Theorems on Factorization and Primality Testing", *Proc. Cambridge Phil. Soc.*, 76 (1974), 521-528.

[31] C. Pomerance, "Are there Counterexamples to the Baillie - PSW Primality Test?", NP, 1994.

[32] C. Pomerance, "The Cyclotomic Ring Test of Agrawal, Kayal and Saxena", Preprint, 2002.

[33] C. Pomerance, J. L. Selfridge and S. Wagstaff, "The Pseudoprimes to $25 \cdot 10^9$", *Math. Comput.* 35 (1980), 1003-1026.

[34] M. Rabin, "Probabilistic Algorithms for Testing Primality", *Journal of Number Theory*, 12 (1980).

[35] H. Rademacher, *Topics in Analytic Number Theory*, Springer-Verlag, New York, 1973.

[36] P. Ribenboim, *The Little Book of Big Primes*, New York, Springer-Verlag, 1991.

[37] P. Ribenboim, *The New Book of Prime Number Records*, New York, Springer-Verlag, 1996.

[38] H. E. Rose, *A Course in Number Theory*, Oxford Press, Oxford, 1994.

[39] M. Rosen, *Elementary Number Theory and its Applications*, Addison Wesley Longman, Ontario. 2000.

[40] W. Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, 1996.

[41] H. Stark, *An Introduction to Number Theory*, Cambridge, MIT Press, eleventh printing, 2001.

[42] Z. H. Sun, "Congruences for Bernoulli numbers and Bernoulli polynomials", *Discrete Math.*, 163 (1997), 153-163.

[43] Z. W. Sun, "General Congruences for Bernoulli Polynomials", *Discrete Math.*, 262 (2003), 252-276.

[44] N. M. Stephens, "On the Feit-Thompson Conjecture." *Math. Comput.*, 25 (1971), 625.

[45] E. W. Weisstein, "Atkin-Goldwasser-Kilian-Morain Certificate", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/Atkin-Goldwasser-Kilian-MorainCertificate.html

[46] E. W. Weisstein, "Bernoulli Number", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/BernoulliNumber.html

[47] E. W. Weisstein, "Bernoulli Polynomial", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/BernoulliPolynomial.html

[48] E. W. Weisstein, "Euler's Factorization Method", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/EulersFactorizationMethod.html

[49] E. W. Weisstein, "Excludent Factorization Method", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/ExcludentFactorizationMethod.html

[50] E. W. Weisstein, "Legendre's Factorization Method", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/LegendresFactorizationMethod.html

[51] E. W. Weisstein. "Miller's Primality Test", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/MillersPrimalityTest.html

[52] E. W. Weisstein. "Prime Diophantine Equations", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/PrimeDiophantineEquations.html

[53] E. W. Weisstein, "Riemann Zeta Function", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/RiemannZetaFunction.html

[54] E. W. Weisstein, "Selfridge-Hurwitz Residue", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/Selfridge-HurwitzResidue.html

[55] E. W. Weisstein, "Vandermonde Matrix", From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/VandermondeMatrix.html

[56] H. C. Williams, "A $p + 1$ Method of Factoring." *Math. Comput.* 39 (1982), 225-234.

[57] E. Wong, "Computations on Normal Families of Primes," *Unpublished.* (SFU Masters Thesis), 1994.

[58] S. Zhang, J. Jin, *Computation of Special Functions*, John Wiley and Sons, Inc, New York, New York. 1996.